



Alliance 8300 Administration Manual and Operation Guide

Copyright	© 2011 UTC Fire & Security. All rights reserved.
Trademarks and patents	<p>Interlogix, the Alliance 8300 name and logo are trademarks of UTC Fire & Security.</p> <p>Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.</p>
Manufacturer	<p>UTC Fire & Security Americas Corporation, Inc. 1275 Red Fox Rd., Arden Hills, MN 55112-6943, USA</p> <p>Authorized EU manufacturing representative: UTC Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, Netherlands</p>
Certification	
Contact information	www.utcfireandsecurity.com or www.interlogix.com
Customer support	www.interlogix.com/customer-support

Content

Important information v

Related documentation v

Typographical conventions vi

System overview 1

Key concepts 2

Setting up Alliance 8300 5

Before you begin 5

Starting Alliance 8300 6

Accessing help 7

Adding an operator 7

Defining facilities 7

Setting system parameters 8

ATS control panel and FAS connections 9

Setting up a network connection to an ATS control panel 9

Setting up a direct connection to an ATS control panel 13

Setting up a dial-up connection to an ATS control panel 15

Setting up a direct connection to a Fire Alarm System 17

Connecting and uploading data 18

Completion 19

Operator interface 20

Introduction 20

Starting Alliance 8300 20

Main window 20

Toolbar 21

Status bar 22

Forms 23

Main menu command reference 24

File Menu 25

Search Menu 27

View Menu 28

Operations Menu 28

Personnel Menu 31

Device Menu 32

Advisor Master menu options [A] 33

Advisor Master > Installer menu options 33

CCTV menu options [C] 41

FAS Menu Options [F] 41

Administration Menu 41

Reports Menu 43

Window Menu 45

Help Menu 45

Setting system parameters 46

Settings tab 46

User Fields tab 49

Address Fields tab 49

Communication Settings tab 49

Clear Archive tab 50

Badge Learn tab 51

Permissions, facilities, and operators 52

Creating Alliance 8300 permissions 52

Creating facilities 54

Creating operators 54

Managing facilities 56

Configuring devices 57

Configuring alarms 57

Configuring a control panel 58

Standard alarm system programming 58

Additional alarm system programming 59

Using a four-door/lift DGP in access control system programming 60

Standard four-door/lift DGP programming 60

Additional four-door/lift DGP programming 62

Configuring DVRs and cameras 63

Access rights, persons, and badges 64

Access rights 64

Person profile 64

Person 65

Badges 65

Badge groups 65

Control panel memory 68

Learning badge data 69

Controlling operations 70

Managing control panels 70

Monitoring badges 72

Monitoring alarms 73

Combined monitoring 74

Creating and using alarm maps 75

Managing clients 76

Managing zones 76

Managing doors 77

Managing high security regions 78

Managing lifts 78

Managing areas 78

Managing arming stations 79

Managing DGPs 79

Managing time locks (TML) 80

Managing Fire Alarm Systems	80
Managing digital video	80
Changing your password	81
Selecting facilities	81
Performing engineer walk test or user walk test	81
Camera footage on alarm	81
Managing network client computers	82
Client Monitor form	82
Client form	83
Reports and templates	84
Reports	84
Standard reports	84
History reports	85
External Reports	86
Templates	86
Print Preview Report	87
Print Report	87
Using Microsoft Access 2002	88
Creating the “exreport” user	88
Setting up MS Access Reports for Alliance 8300	90
Launching External Reports from Alliance 8300	94
MS Access 2002 database utilities	95
Database and system management	96
Overview	96
Alliance 8300 databases	96
Alliance 8300 files and settings	101
Restoring data from a backup	103
System recovery	105
Diagnostics and troubleshooting	107
Turning on diagnostics	107
Creating a Logfile	107
Viewing the diagnostics logs	108
Questions and answers	109
Installing Alliance 8300	109
Using Alliance 8300	112
Hardware	115
Server-client communications	116
Uninstalling Alliance 8300	117
Appendix A. CCTV Support	118
Introduction	118
Setup and configuration	118
Digital Video Recorders (DVRs)	118

Appendix B. Changing the server name 119

Introduction 119

Changing the name in Windows 119

Changing the name in Windows registry 120

Changing the name in the Alliance 8300 database 121

Changing the name in ODBC 121

Appendix C. Adding windows users to Alliance 8300 125

Introduction 125

Adding Windows users 126

Appendix D. Configuring file sharing 129

Appendix E. Managing passwords 130

Introduction 130

Windows user passwords 130

Database passwords 132

Resetting the application password 134

Appendix F. Alliance 8300 utilities 137

Introduction 137

Database utilities 137

System administration utilities 139

Index 145

Important information

The *Alliance 8300 Administration Manual* is a comprehensive guide to Alliance 8300 for both the system administrator and the installation technician to program, configure, and use the Alliance 8300 system. It supplements and expands the operator information contained in the *Alliance 8300 Online Help* and provides a level of detail required by advanced operator such as system administrators and installation technicians.

This manual does not describe how to plan and structure an entire security and access control system — it describes only how to manage the operation of Alliance 8300 in an existing security and access control system.

It is assumed that the security and access control system is in place and Alliance 8300 client and server computers have been installed and licensed in accordance with the *Alliance 8300 Installation Manual*.

It is further assumed that users of this manual have read and understood the *Alliance 8300 Installation Manual*.

Related documentation

For more information, refer to the following documentation.

Other manuals

- *Alliance 8300 Installation Manual*: Provides information for Integration Technicians to set up, install, and configure an Alliance 8300 system.
- *Alliance 8300 Imaging User Guide*: Provides instructions for users of the optional Imaging package.
- *Alliance 8300 CCTV Interface Guide*: Provides interface instructions for CCTV equipment.
- *Alliance 8300 FAS Reference Guide*: Provides setup instructions for Fire Alarm Systems.
- *Alliance 8300 API Manual*: Alliance 8300 API (Application-Program Interface) provides the ability to import data from external applications such as a Human Resource Management System.
- *Alliance 8700 Installation Manual*: Provides information for Integration Technicians to set up, install, and configure Alliance 8700 Smart Card Programmer software.
- *DVMRe User Manual*: Not supplied with Alliance 8300.
- *SymSafe, SymSafe PRO & SymDec User Manual*: Not supplied with Alliance 8300.
- *DVSR User Manual*: Not supplied with Alliance 8300.

Online help

- *Alliance 8300 Online Help*: Provides reference information, such as screen and field descriptions, along with instructions for system administrator duties, such as configuring Alliance panels.
- *Alliance 8300 License Setup Online Help*: The Alliance 8300 License Setup application is used to register the Alliance 8300 License to enable communications with client computers and to enable the Image Capture and GuardDraw applications.
- *Alliance 8700 Online Help*: Provides reference information, such as screen and field descriptions for the Alliance 8700 Smart Card Programmer software.
- *Image Capture Online Help*: The Capture application is used to add an image or signature to a Person form.
- *GuardDraw Online Help*: The GuardDraw application is used to create and edit badge designs.
- *Digital Video Viewer Online Help*: The Digital Video Viewer application is used to monitor digital video multiplexers/recorders and their associated cameras, control live video, as well as search and play back recorded video events.
- *Digital Video Recorder Search Online Help*: The Digital Video Search application is used to search for recorded video events triggered by reader and/or alarm transactions.
- *Diagnostic Viewer Online Help*: The Diagnostic Viewer application is a diagnostic tool used to view the contents of Alliance 8300's diagnostic log files, apply filters to limit the information displayed, and search for a specific log entry.

Typographical conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

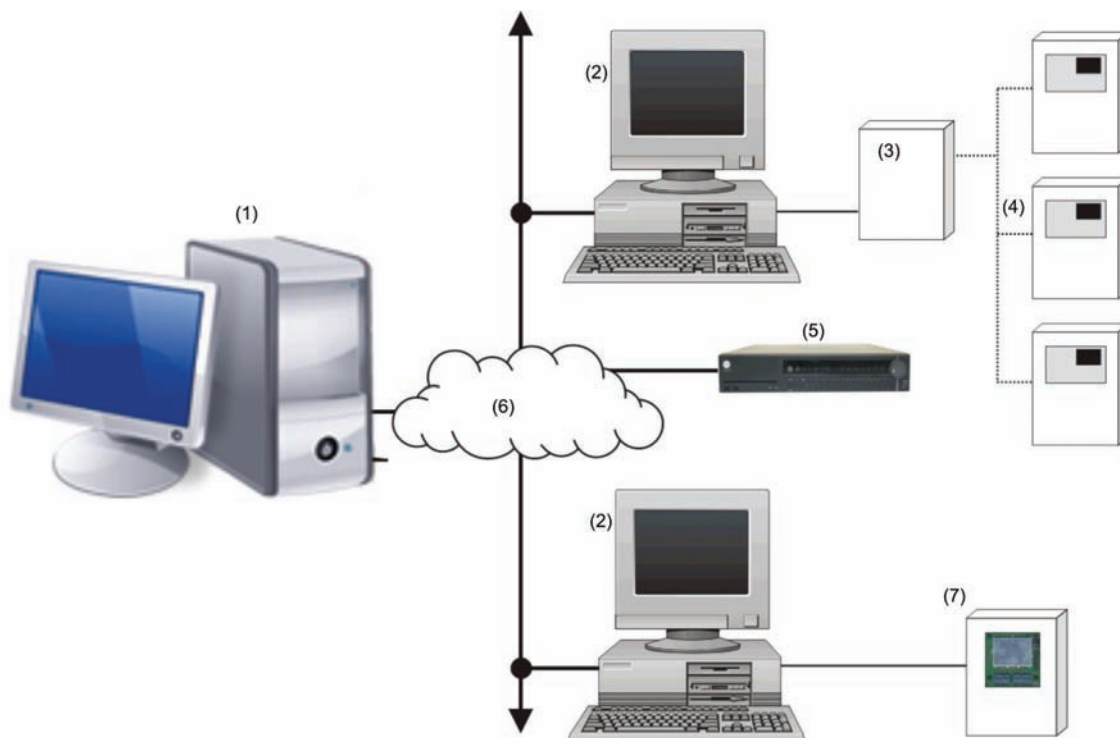
Item	Description
Command sequences	Where appropriate, command sequences are abbreviated with the ">" symbol. For example, the command "Click Start, and then click Run" is written as "Click Start > Run".
Command alternatives	Many commands can be executed in a variety of ways including menu bar, tool bar, shortcut keys, right click, or double click. In general, commands are described from their menu bar location only, even when alternatives exist.
Keys	Capitalized, for example "press Enter".
Keystrokes	Text that you type is indicated in Courier New font. For example, "Type dcomcnfg".
Expanding a "tree" view	The word "expand" is used to indicate that selections may be hidden. For example, the command "Click the '+' box next to Computers" is written as "Expand Computers".

Item	Description
Notes	Notes alert you to information that can save you time and effort.
Caution	Cautions are displayed to advise the user that failure to take or avoid a specified action could result in loss of data.
[F]	This letter indicates that the action or option described is specific to the fire equipment (FAS).
[A]	This letter indicates that the action or option described is specific to the intrusion and access control equipment (ATS).
[C]	This letter indicates that the action or option described is specific to the CCTV equipment.

System overview

Alliance 8300 is a client-server security system management application with the ability to communicate over a LAN or WAN. Figure 1 below depicts the relationship between an Alliance 8300 server and remote Alliance 8300 clients.

Figure 1: Alliance 8300 Professional Edition with two remote clients and a digital video recorder



(1) Alliance 8300 Professional Server

Professional Server components:

- Alliance 8300 Client (user interface)
- Alliance 8300 Databases
- Alliance 8300 Imaging (optional application)
- Alliance 8300 Diagnostics (service)
- Alliance 8300 System Manager (service)
- Alliance 8300 Manager (service)
- MS SQL (service)

(3) Global fire repeater

(4) Fire panel network

(5) DVR

(6) Ethernet TCP/IP, LAN or WAN*

(7) ATS control panel

(2) Alliance 8300 Client PC

Client computer components:

- Alliance 8300 Client (user interface)
- Alliance 8300 Imaging (optional application)
- Alliance 8300 Diagnostics (service)
- Alliance 8300 System Manager (service)
- Alliance 8300 Manager (service)

*WAN data transfer latency can significantly reduce the Alliance applications usability.

Key concepts

This section discusses the key concepts that you need to consider when using Alliance 8300, in particular the differences from other security management systems that you may be familiar with.

Badge groups [A]

The purpose of badge groups is to provide flexibility in setting up multi-panel security systems where some panels must cater for a large number of users (such as a main entrance) and other panels that cater for smaller numbers of users (such as individual departments on different floors).

Badge Groups are based on Badge Formats, as listed in “Badge groups” on page 65, or custom formats. After creating a new badge group, assign the badge group to a control panel via the Badge Groups tab on the Controller Setup form.

Here is an example of how a combination of large and small control panels in the same system can be handled by managing badge groups:

- Control panel A controls the building’s main entrance and it has a memory size of IUM large (Intelligent User Module), which enables the control panel to handle up to 65,535 users.
- Control panel B controls the building’s administration offices and it has no memory expansion (up to 50 users). A special Badge Group has been created and assigned to Control panel B named Administration Staff. Whenever a change occurs in Alliance 8300 to a person’s record or access rights assigned to the Administration Staff, Alliance 8300 automatically downloads (sends) the required user data to Control panel B.
- Control panel C controls the building’s engineering offices and also has no memory expansion (up to 50 users). A special Badge Group has been created and assigned to Control panel B named Engineering Staff. Whenever a change occurs in Alliance 8300 to a person’s record or access rights assigned to the Engineering Staff, Alliance 8300 automatically downloads (sends) the required user data to Control panel C.
- Control panel A has been assigned the Badge Groups Administration Staff and Engineering Staff (among others). Whenever a change occurs in Alliance 8300 to a person’s record or access rights belonging to either the Administration Staff or the Engineering Staff, Alliance 8300 automatically downloads (sends) the required user data to Control panel A (as well as to Control panel B or Control panel C, as needed).

For more information see “Badge groups” on page 65 and “Control panel memory” on page 68.

Controller setup [A]

All new Alliance 8300 control panel records are created with at least one MASTER badge group:

- Master Installer type (assigned Badge No. 50) enables a new control panel to be programmed initially.

- Master User type (assigned Badge No. 1) enables a new control panel to be used for access initially. The Master User type does not apply to Australian database defaults.

See “Master badge groups” on page 66 for details.

Caution: Before saving a new record for a control panel with existing users, remove the MASTER badge groups to avoid overwriting users 1 and 50. Refer to “Assigning badge groups” on page 67 for details.

Person profiles [A]

Person profile records are defined in Alliance 8300 from the Personnel > Person Profile menu entry.

Person profiles control permissions. A Person profile is the name given to a particular category of person (such as “Office Staff”), which share a set of access rights. Access rights are determined by up to three access groups (Alarm group, Door group, and Floor group).

Persons [A]

Person records are defined in Alliance 8300 from the Personnel > Person menu entry.

A Person record contains details about a potential* user of the security system and assigns a Person Profile to provide the appropriate access rights.

*A potential user becomes a user when a badge (or PIN) is assigned via the Badge form.

Badges [A]

In Alliance 8300, the term “badge” can refer to a:

- Smart card or key fob
- Magnetic stripe card
- PIN
- Combination of card and PIN

In other words, a badge may be a physical device, a number entered at a keypad, or both.

It is the badge data that is downloaded to a control panel.

See “Badges” on page 65 for more information.

Facilities [A] [F]

Facility records are defined in Alliance 8300 from the Administration > Facility menu.

It is recommended that you create facilities and associate new control panels (ATS or FAS) to facilities from the very start (assign a facility to a control panel record before saving the record). This will help ensure that all the data related to the control panel is kept within the same database partition and will help speed access to data.

Note: After a control panel has an assigned facility, uploaded devices for the control panel will automatically be assigned to the same facility.

Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, operators assigned with a permission of System Administrator are assigned to all facilities. All records have the default Ignore Facilities, which means the records are not under facility protection; therefore, those records are visible to all operators.

Creating and using facilities are separate things:

- To create a facility, use the Facility tab on the Facility form.
- To assign a facility to the required operator, use the Facilities tab on the Operator form.
- To manage a facility's state, use the Operations > Select Facilities command. Facilities assigned to an operator are active by default. A facility may be set to "Available" (inactive) when it's not needed. For example, a facility may be created for future use and then made inactive to prevent the facility from being accidentally selected by the operator when using various forms.

Note: If you, as an operator, do not have a particular facility assigned to you, that facility will not be available to you from the Facilities list on various forms.

Event-triggered video [C]

Event-triggered video records are defined in Alliance 8300 from the Administration > Event Trigger menu entry.

Event triggers allow you to move up to four PTZ (pan tilt zoom) cameras into pre-set positions in response to specific door/reader transactions and/or alarm transactions.

This function can be used, for example, to obtain a video image at a door if someone attempts entry using a badge that has been identifies as 'lost', or if an intrusion or a fire alarm is generated. In addition, a tag can be automatically sent to the DVR for marking the recorded video and for changing the camera's recording rate appropriately.

Refer to the *Alliance 8300 CCTV Interface Guide* for more information.

Setting up Alliance 8300

This chapter describes how to set up Alliance 8300 to a minimum degree in order to connect to a control panel and to upload data.

Once you have installed the Alliance 8300 software on the server and clients (if applicable), you will need to log in to the server computer and set a few parameters.

Before you begin

Information you will need

As part of the task of integrating Alliance 8300 into an existing security and access control system there are a number of issues that you'll need to consider. It will save time if you prepare or obtain this information before sitting down in front of Alliance 8300 and having to think about it as you come to it. The main issues are as follows:

- **Permissions:** In addition to the default System Administrator what operator permission categories will you need?
- **Operators:** In addition to the default Alliance 8300 operator login secure what operators will you need? (The default Alliance 8300 operator has System Administrator operator permission.)
- **Access Rights [A]:** Access Rights are defined by Person Profiles. In addition to the default Master Installer Profile what access rights definitions will you need?
- **Windows Users:** See "Appendix C. Adding windows users to Alliance 8300" on page 125 for information about setting up Windows users.
- **File sharing:** Simple File Sharing model in Windows must be set to Classic. See "Appendix D. Configuring file sharing" on page 129.
- **Facilities:** A facility is a way to organize records in the Alliance 8300 database by, for example, a location. See also "Defining facilities" on page 7.
- **Personnel Types [A]:** In addition to the default Permanent, Contractor, and Temporary, what personnel types will you need? A personnel type can be associated with a specific badge design.
- **Badge Designs [A]:** Default badge designs are provided as a starting point but must be edited to suit your needs. A badge design can be associated with personnel types so that, for example, you can tell from the badge which staff are permanent and which are contractors. Alliance 8300 workstations require Imaging to be installed and licensed in order to edit badge designs.
- **Department [A]:** Department names are used in person records and reports for sorting purposes.
- **Badge Groups [A]:** Alliance 8300 provides several default badge groups for use with control panels. It is recommended that you determine what badge

groups are needed for each new control panel defined in Alliance 8300 and remove unneeded badge groups before you initially save the control panel record. Refer to the *Alliance 8300 Online Help* for more information.

Tasks to be performed

Table 2 below describes the Alliance 8300 tasks required to verify that the Alliance 8300 installation is complete and functioning correctly.

Table 2: Initial Setup of Alliance 8300

Task	Menu > Form	Reference
1. Start Alliance 8300 and log in	File > Login	page 6
2. Add yourself as an operator in Alliance 8300	Administration > Operator	page 7
3. Program system parameters	Administration > Parameters	page 8
4. OPTIONAL: Create facilities	Administration > Facility	page 7 See also the <i>Alliance 8300 Online Help</i> .
5. Add the client computers to the Alliance 8300 server computer database	Administration > Client	See <i>Adding Alliance 8300 Clients</i> in the <i>Alliance 8300 Installation Manual</i> .
6. Set up client computers	Not applicable	This table
7. Connect to a control panel	Operations > Controller Utility	page 9
8. Retrieve data from the control panel	Right click > Upload	page 17

For information on advanced setup topics see the *Alliance 8300 Online Help*.

Starting Alliance 8300

To start Alliance 8300:

1. Select Start > Programs > UTC Fire & Security > Alliance 8300 > Alliance 8300 to run the application. Alternatively, double click the Alliance 8300 desktop icon.



2. On the Alliance 8300 menu, select File > Login. Use the default Login ID 'secure' and previously defined password to log in.

Note: In order to log into Alliance 8300 from a client computer:

- You must have a valid Windows user name and password, which is part of the AllianceGroup local group on the Alliance 8300 server computer.

- You must have a valid Alliance 8300 operator login ID and password.
- Alliance 8300 on the server computer must be licensed.
- The database services on the server computer must be running (the easiest way to ensure this is to have Alliance 8300 running on the server computer).

Accessing help

To access the Online Help, press the F1 key. Alternatively, select Help > Help Topics. from the menu bar.

Note: You do not have to be logged in to access help.

Adding an operator

Add yourself as an operator in Alliance 8300. This will allow Alliance 8300 to record the steps you take in setting up the system.

To add yourself as an operator in Alliance 8300:

1. Select Administration > Operator.
2. Select File > New Record. The Operator form displays in edit mode (the Save Record command is enabled).
3. Add your details to the Operator form. Various permissions are available initially referring to certain tasks (like security, reception or System Administrator). Select an appropriate permission.

For detailed information about setting up an operator, refer to the *Alliance 8300 Online Help*.

4. Save the Operator form, log off, and then log in as the new operator.

Defining facilities

The Alliance 8300 database can be partitioned and related records can be grouped. In Alliance 8300, these groups are called facilities. A Facility option can be designated on most forms throughout the system and any number of facilities can be defined.

It is recommended to create facilities and associate new control panels to facilities from the very start (assign a facility to a control panel record before saving the record). This will help ensure that all the data related to the control panel is kept within the same database partition and will help speed access to data.

Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, the system administrator is assigned to all facilities. All records have the default Ignore Facilities, which means the records are not under facility protection; therefore, those records are visible to all operators.

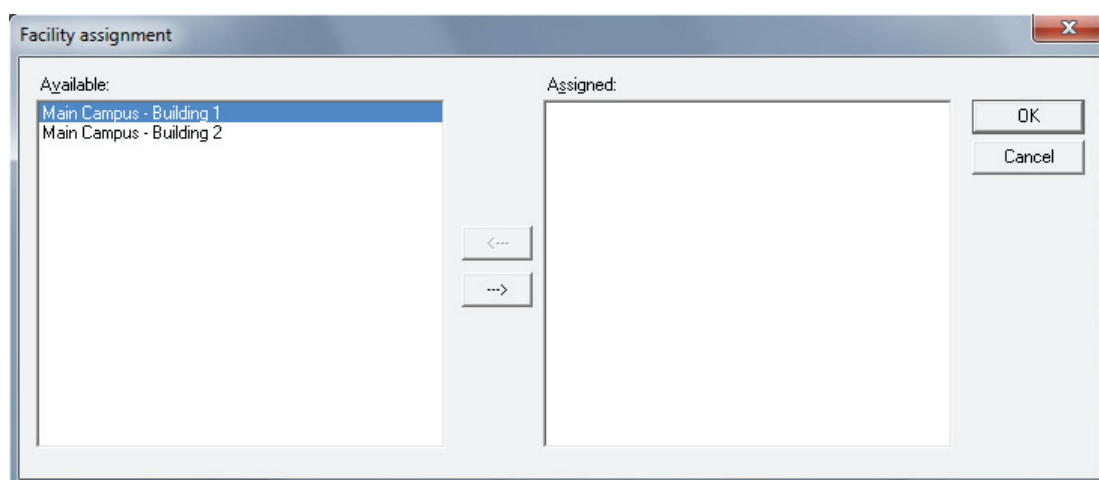
For more information about setting up a facility, refer to the *Alliance 8300 Online Help*.

You can assign more than one facility to an operator.

To assign the operator to a facility:

1. Click Administration > Operator.
2. Click Search > Search to display the operator records.
3. Select the operator to which you want to assign to a facility. (If only one operator record was created, it will be displayed.)
4. Click the Facilities tab.
5. Click Assign Facilities.

Result: The Facility Assignment dialog displays.



In this example there are two facilities available: Main Campus—Building 1 and Main Campus — Building 2. We want to assign an operator to the Main Campus — Building 1 to allow the operator to assign badge holders to that facility only.

6. In the Available column, select the facility that you want to assign to the operator.
7. Click the right arrow button to move the selection to the Assigned column.
8. Click OK. In the given example the facility Main Campus — Building 1 now displays in the Assigned column.
9. Click File > Save Record to save the changes.

Setting system parameters

System settings for Alliance 8300 are determined by the Parameters form. On the Parameters form, you can specify, among others:

- To archive history on a specific time interval, such as daily, weekly, or monthly; or to archive history immediately
- To print badge and alarm activity and to which printers

- To change the names of the labels that will be used globally for the user fields and address fields, etc.

Note: For the changes on the Parameters form to take effect, you **MUST** save the change and then stop and restart the Alliance 8300 services. The easiest way to do this is to restart the computer.

For more information on these items, refer to the *Alliance 8300 Online Help*.

ATS control panel and FAS connections

When an Alliance 8300 computer is connected to a controller (control panel), the computer is said to be the host of the controller. The details of the controller and its connection to the host are defined by an Alliance 8300 controller record.

Note: When creating controller records, it is recommended to avoid using a host computer that is likely to have its computer name changed. Any Alliance 8300 computer (server or client) that has had its computer name changed will lose communication with all controllers hosted by that computer. In such a case, the controller records for affected panels would have to be deleted and then recreated using the new computer name.

The Alliance 8300 computer may be connected to a controller (ATS control panel or Fire alarm system) in the following ways:

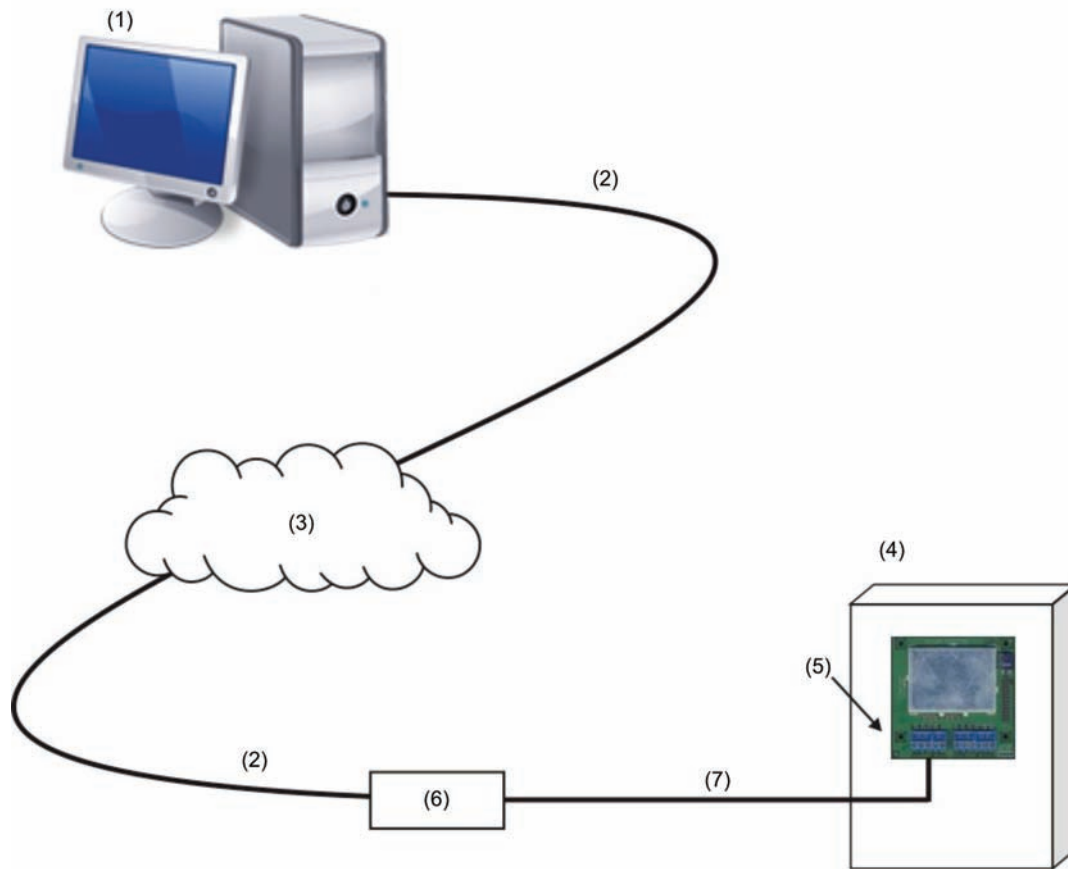
- ATS control panel:
 - Network (Ethernet) connection to 8- or 16-area control panels. See “Setting up a network connection to an ATS control panel” below for details.
 - Direct connection. See “Setting up a direct connection to an ATS control panel” on page 13 for details.
 - Dial-up connection via modem. See “Setting up a dial-up connection to an ATS control panel” on page 15.
- Fire alarm system:
 - Direct connection. See “Setting up a direct connection to a Fire Alarm System” on page 17 for details.

Setting up a network connection to an ATS control panel

The Advisor Master control panel fitted with a suitable Ethernet adaptor such as the ATS1806 Universal Interface can be connected via Internet Protocol (IP) to the Alliance 8300 computer via a LAN or WAN to provide control and upload and download capabilities.

Note: The ATS1806 Universal Interface supports IP connection up to 10 Mbps.

Figure 2: Ethernet connection via ATS1806 Universal Interface and ATS1801 Computer-Printer Interface



(1) Alliance 8300 Computer
Static IP Address (for example,
3.248.65.2)
Port (for example, 3001)

(2) Category 5 cable

(3) Ethernet TCP/IP, LAN or WAN

(4) Control panel

(5) Computer-Printer Interface (Port A)

(6) Universal Interface
Static IP Address (for example,
3.248.65.3)

Port (for example, 3001)

(7) RS232

The Advisor Master control panel must be fitted with the following devices to provide a network connection:

- ATS1801 Computer-Printer Interface is fitted to the Advisor Master control panel.
- ATS1806 Universal Interface connects to the RS232 port A on the ATS1801 Computer-Printer Interface. The ATS1806 Universal Interface has an RJ45 Ethernet port for network connection.

In addition to providing a network connection between the Alliance 8300 computer and an Advisor Master panel, the ATS1806 Universal Interface has a web interface to enable programming of the Alliance panel's communication settings. This web interface may be accessed via Internet Explorer on the Alliance 8300 computer.

Prerequisite data — Alliance 8300 computer

You need the following details about the Alliance 8300 computer:

- IP address
- Port number

The network administrator may need to provide these details.

The Alliance 8300 computer must be connected to the network (i.e. the network is visible to the Alliance 8300 computer's web browser).

Prerequisite data — control panel

You need the following details about the control panel:

- Model (for example, ATS4003).
- Memory size (for example, IUM Large).
- Computer address (for example, 27).
- Password (for example, 0123456789).
- Encryption Key (if used). See "Using encryption keys" on page 13 for details.

Use a RAS to interrogate the control panel for computer address and password, also ensure that the setting for Security Attempts will allow communications.

If the password displayed in the Password field of the Controller Setup form is not correct, you must change the password in the Computer Connections Setup form. Refer to *Alliance 8300 Online Help* for details.

Prerequisite data — Universal Interface

You need the following details about the Universal Interface:

- Port number (for example, 3001)
- IP address
- User name
- Password

The Universal Interface must be connected to the network. You should see "Welcome to the Universal Interface" after you enter the Universal Interface's IP address at the browser's address bar (for example, <http://3.200.65.201/>) on the Alliance 8300 computer.

Setting up the Universal Interface

See the *ATS1806 Universal Interface Installation and Programming Guide* for details about installing and programming the Advisor Master panel's Universal Interface.

Use the following process to set up a network connection between the Alliance 8300 computer (the Universal Interface uses the term "central station") and a Universal Interface connected to an Advisor Master control panel.

To configure the Universal Interface to accept commands from the Alliance 8300 computer:

1. Use a web browser to log on to the Universal Interface at the Universal Interface's IP address.

2. In Central Station Parameters, for one of the station numbers 4 through 10, specify a single Alliance 8300 computer's parameters for:

- IP address
- Protocol (select UDP)
- Port number
- Event type (select Computer)
- Encryption (select Twofish if required)

Note: Alarm Reporting Central Stations 1 to 3 are used for reporting to the Central Stations or for the Secure Stream. Management Central Stations 4 to 15 are used for communication to Alliance 8300.

3. Click the Submit button to save the changes.
4. Click Restart Communications to apply the changes.

Setting up Alliance 8300

To log in to Alliance 8300 and define the control panel:

1. In Alliance 8300, select Device > Advisor Master > Setup. The Controller Setup form displays in search mode (the Save Record command is disabled).
2. Select File > New Record. The Controller Setup form displays in edit mode (the Save Record command is enabled).
3. Type a description (a name) to identify the control panel.
4. Click the Facility arrow and select the facility that the control panel will belong to. See "Facilities [A] [F]" on page 3 for details about facilities.
5. On the Definition tab, define the control panel (for more information, press F1 for online help).
6. On the Communications tab, click the Communication Type arrow and select IP.
7. Under IP Settings, specify the IP address and the port number of the Advisor Master control panel.
8. Type the Encryption Key (if used) in the 16 encryption key fields. See "Using encryption keys" on page 13 for details.
9. If the control panel and the Alliance 8300 computer are located in different time zones, click the Timezone tab to select the control panel's time zone.
10. If the control panel already has existing users, click the Badge Groups tab, and then remove any Badge Groups named MASTER Installer Type or MASTER Operator Type.

Note: Failure to remove Badge Groups named MASTER Installer Type or MASTER Operator Type prior to saving a new control panel record may result in overwriting existing users 1 and 50 with the MASTER Installer or MASTER Operator types (as applicable).

11. Select File > Save Record.

Note: Prior to connecting to a control panel for the first time you may wish to suppress the receiving of events. See “Connecting and uploading data” on page 18 for details.

Using encryption keys

When setting up a connection to a control panel, you have two options regarding encryption:

- Establish communications without using encryption. In this case, troubleshooting a failed connection may be easier because you don't have an incorrect encryption key as a potential fault. However, some steps will need to be repeated to set up encryption in both Alliance 8300 and the Universal Interface after communications have been established.
- Use encryption from the outset. In this case, troubleshooting a failed connection may be more difficult because you have the 16 encryption key fields to check in both Alliance 8300 and the Universal Interface. This is the more secure option because unencrypted control panel data is not transmitted over the network.

Setting up a direct connection to an ATS control panel

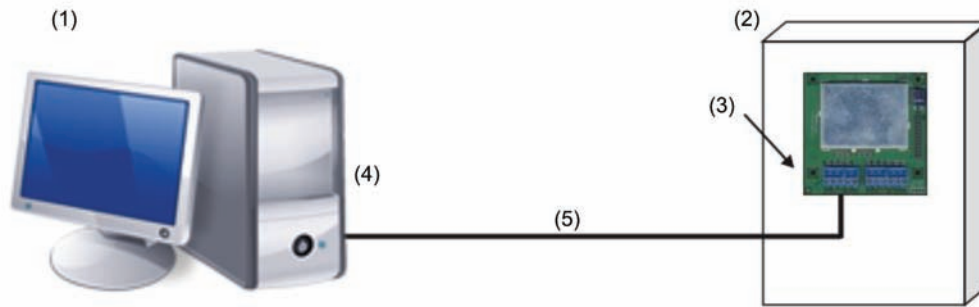
An Alliance 8300 computer may connect directly to the Advisor Master control panel fitted with a ATS1801 Computer-Printer Interface. The Alliance 8300 computer's serial COM port connects to the RS232 port A on the Computer-Printer Interface.

Alternatively, a control panel's RS232 service port (J18) may be used for a temporary connection to the Alliance 8300 computer. Refer to the *Alliance 8300 Online Help* for details.

Multiple control panels may be connected to the same serial port (multidrop) by using a combination of RS485 LAN to Isolated RS232 Interfaces, such as ATS1741. Reduced communication speed may prohibit the use of multidrop with large capacity systems.

Note: For best performance, every control panel should be connected to a corresponding serial port on the Alliance 8300 computer.

Figure 3: Direct connection via ATS1801 Computer-Printer Interface



- | | |
|---|-------------------------------------|
| (1) Alliance 8300 Computer | (4) Serial port (for example, COM1) |
| (2) Control panel | (5) RS232 |
| (3) Computer-Printer Interface (Port A) | |

Prerequisite data — Alliance 8300 computer

You need to know the COM port number for the Alliance 8300 computer.

Prerequisite data — control panel

You need the following details about the control panel:

- Model (for example, ATS4003)
- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)

Use a RAS to interrogate the control panel for computer address and password, also ensure that the setting for Security Attempts will allow communications.

Use the following process to set up a direct connection between the Alliance 8300 computer and an Advisor Master control panel.

Setting up Alliance 8300

To define the Advisor Master control panel:

1. In Alliance 8300, select Device > Advisor Master > Setup. The Controller Setup form displays in search mode (the Save Record command is disabled).
2. Select File > New Record. The Controller Setup form displays in edit mode (the Save Record command is enabled).
3. Type a description (a name) to identify the control panel.
4. Click the Facility arrow and select the facility that the control panel will belong to. See “Facilities [A] [F]” on page 3 for details about facilities.
5. On the Definition tab, define the control panel (for more information, press F1 for online help).

6. On the Communications Settings tab, click the Communication Type arrow and select Serial.
7. Under Serial / Dial-Up, click the Com Port arrow and select the port that will be used to connect to the control panel.
8. If the control panel and the Alliance 8300 computer are located in different time zones, click the Timezone tab to select the control panel's time zone.
9. If the control panel already has existing users, click the Badge Groups tab, and then remove any Badge Groups named MASTER Installer Type or MASTER Operator Type.

Note: Failure to remove Badge Groups named MASTER Installer Type or MASTER Operator Type prior to saving a new control panel record may result in overwriting existing users 1 and 50 with the MASTER Installer or MASTER Operator types (as applicable).

10. Select File > Save Record.

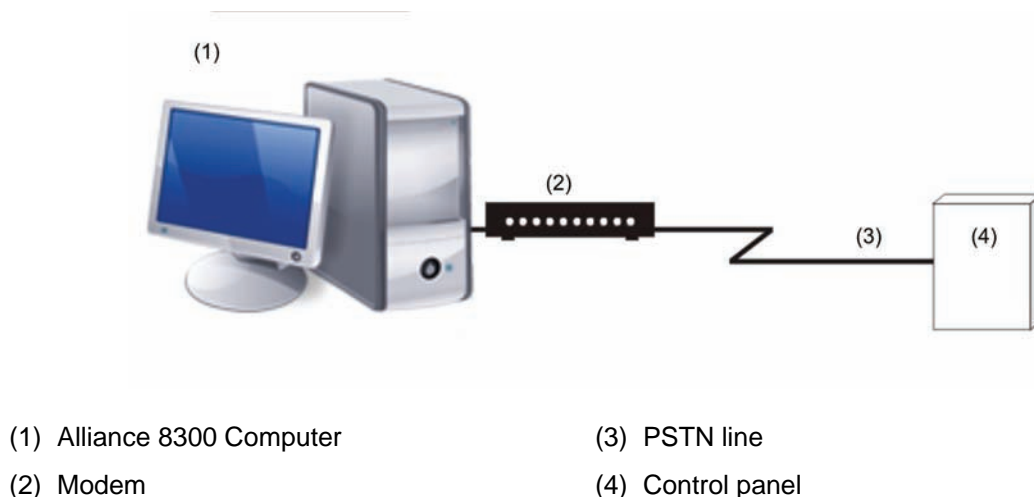
Note: Prior to connecting to a control panel for the first time you may wish to suppress the receiving of events. See "Connecting and uploading data" on page 18 for details.

Setting up a dial-up connection to an ATS control panel

An Alliance 8300 computer fitted with an approved modem may connect to a control panel via dial-up.

Note: If a modem is to be used to communicate with a control panel, you must manually lock the speed of the modem at 300 baud.

Figure 4: Dial-up connection via modem



Prerequisite data — Alliance 8300 computer

You need to know the telephone number of the modem that the Alliance 8300 computer will use for connecting with dial-up control panels.

Prerequisite data — control panel

You need the following details about the control panel:

- Model (for example, ATS4003)
- Memory size (for example, IUM Large)
- Computer address (for example, 27)
- Password (for example, 0123456789)
- Phone number

Use a RAS to interrogate the control panel for computer address and password, also ensure that the setting for Security Attempts will allow communications.

Use the following process to set up a dial-up connection between the Alliance 8300 computer and an Advisor Master control panel.

Setting up Alliance 8300

Note: You must program the modems to be used by the Alliance 8300 system in the Parameters form > Communications Setting tab, and then restart the Alliance 8300 server for the settings to be in effect. Refer to the *Alliance 8300 Online Help* for details.

To define the Alliance control panel:

1. In Alliance 8300, select Device > Advisor Master > Setup. The Controller Setup form displays in search mode (the Save Record command is disabled).
2. Select File > New Record. The Controller Setup form displays in edit mode (the Save Record command is enabled).
3. Type a description (a name) to identify the control panel.
4. Click the Facility arrow and select the facility that the control panel will belong to. See “Facilities [A] [F]” on page 3 for details about facilities.
5. On the Definition tab, define the control panel (for more information, press F1 for on-line help).
6. On the Communications tab, click the Communication Type arrow and select Dial-Up.
7. On the Dial Settings tab, type the phone number of the dial-up control panel.
8. Select the other Dial Settings options, as needed (for more information, press F1 for online help).
9. If the control panel and the Alliance 8300 computer are located in different time zones, click the Timezone tab to select the control panel’s time zone.
10. If the control panel already has existing users, click the Badge Groups tab, and then remove any Badge Groups named MASTER Installer Type or MASTER Operator Type.

Note: Failure to remove Badge Groups named MASTER Installer Type or MASTER Operator Type prior to saving a new control panel record may result in overwriting existing users 1 and 50 with the MASTER Installer or MASTER Operator types (as applicable).

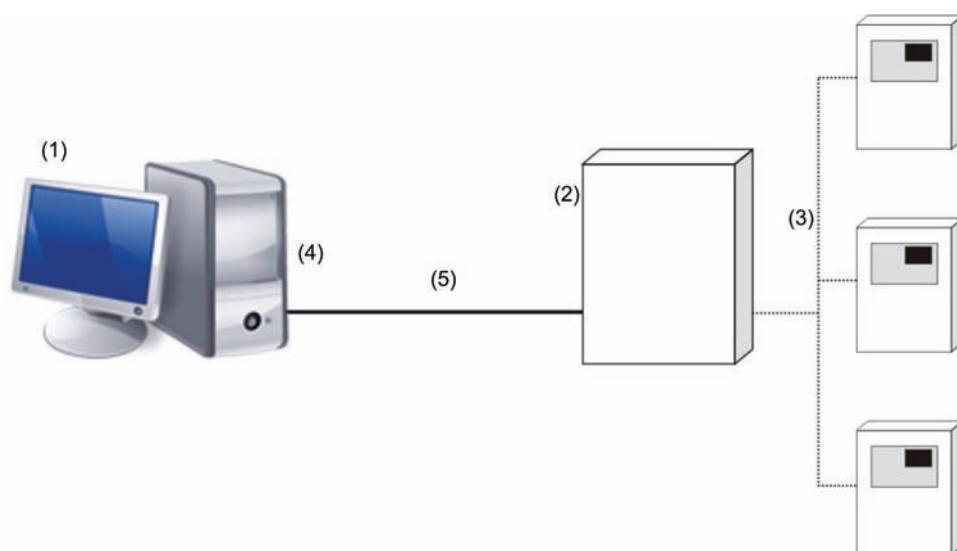
11. Select File > Save Record.

Note: Prior to connecting to a control panel for the first time you may wish to suppress the receiving of events. See “Connecting and uploading data” on page 18 for details.

Setting up a direct connection to a Fire Alarm System

An Alliance 8300 computer may be connected directly to the Fire Alarm System device. This can be a Fire panel or a Global repeater.

Figure 5: Direct connection to FAS



(1) Alliance 8300 Computer

(4) Serial port (for example, COM1)

(2) Global repeater

(5) Null-modem

(3) Fire panels network

Prerequisite data — Alliance 8300 computer

You need to know the COM port number for the Alliance 8300 computer.

Prerequisite data — FAS system

You need the following details about the fire alarm system:

- Serial connection baud rate (default is 9600 bps)
- FAS network addressing mode
- Host address (the address of the Alliance host computer in the FAS network)
- FAS network structure (networked panels and global repeaters addresses)
- FAS access code

Use global repeater keypad or specific FAS configuring software to program the PC communication for FAS, also ensure that all necessary FAS network nodes are programmed to communicate to the Alliance host computer.

Use the following process to set up a direct connection between the Alliance 8300 computer and a FAS.

Setting up Alliance 8300

To define FAS:

1. In Alliance 8300, select Device > FAS > Setup. The FAS Setup form displays in search mode (the Save Record command is disabled).
2. Select File > New Record. The FAS Setup form displays in edit mode (the Save Record command is enabled).
3. Type a description (a name) to identify the FAS.
4. Click the Facility arrow and select the facility that the FAS will belong to. See “Facilities [A] [F]” on page 3 for details about facilities.
5. On the Communications tab, click the Host Computer arrow and select the computer the FAS is connected to.
6. Under Serial connection, select the COM port and a baud rate for FAS connection.
7. In the Password panel, enter the global repeater or the panel access code and confirm it.
8. In the FAS Network tab, select Addressing mode, Host address, and choose all necessary FAS network nodes communicating with Alliance host computer (for more information, press F1 for on-line help).
9. If the FAS and the Alliance 8300 computer are located in different time zones, click the Timezone tab to select the control panel’s time zone.
10. Select File > Save Record.

Note: Prior to connecting to FAS for the first time you may wish to suppress the receiving of events. See “Connecting and uploading data” below for details.

Connecting and uploading data

You must upload (retrieve) a database from a control panel for the first time.

To upload a database from a control panel:

1. Select Operations > Controller Utility. The Controller Utility form displays with the new control panel listed.

Note: Suppress receiving events from the control panel until after uploading the full database. This enables Alliance 8300 to learn details of the alarms to be reported, and so avoids the alarms being lost and reported as warnings in the diagnostic log.
2. Right click the control panel in the Controller Utility form and clear the Accept Events option to suppress receiving events from the control panel.
3. Right click the FAS or the control panel in the Controller Utility form and select Set Online. Alliance 8300 initiates communication with the device. After communication has been established, the status field displays Connected.

4. Right click the FAS or the control panel in the Controller Utility form and select Upload > Full Database to copy the entire database from the controller into Alliance 8300.
5. If you suppressed events in step 2, you may now select the Accept Events option if you want to receive events.

Completion

After connecting to a control panel and uploading data, you have verified the operation of Alliance 8300. This concludes the installation process.

Operator interface

Introduction

This chapter describes the Alliance 8300 workspaces and the methods of selecting operator commands.

The Alliance 8300 login ID identifies an operator, and every operator has assigned permissions to use various Alliance 8300 menu items. There may be menu items described in this chapter that a particular operator does not have permission to use, or the use might be restricted to read-only.

In addition to possible restriction over menu options, an operator's use of Alliance 8300 may be further restricted by the application of facilities. For example, an operator responsible for facilities A and B will not see control panels, devices, or various transactions associated with facility C.

Where permission defines access rights to the menu items, facilities provide a filter on data shown in the forms related to menu items.

The use of permissions and facilities enables an Alliance 8300 operator to work with only the items that may require the operator's attention.

Starting Alliance 8300

1. Select Start > Programs > UTC Fire & Security > Alliance 8300 > Alliance 8300 to run the application. Alternatively, double click the Alliance 8300 desktop icon.



2. On the Alliance 8300 menu, select File > Login. Use the default Login ID "secure" and the assigned password to log in, or use your assigned login ID and password (if applicable).

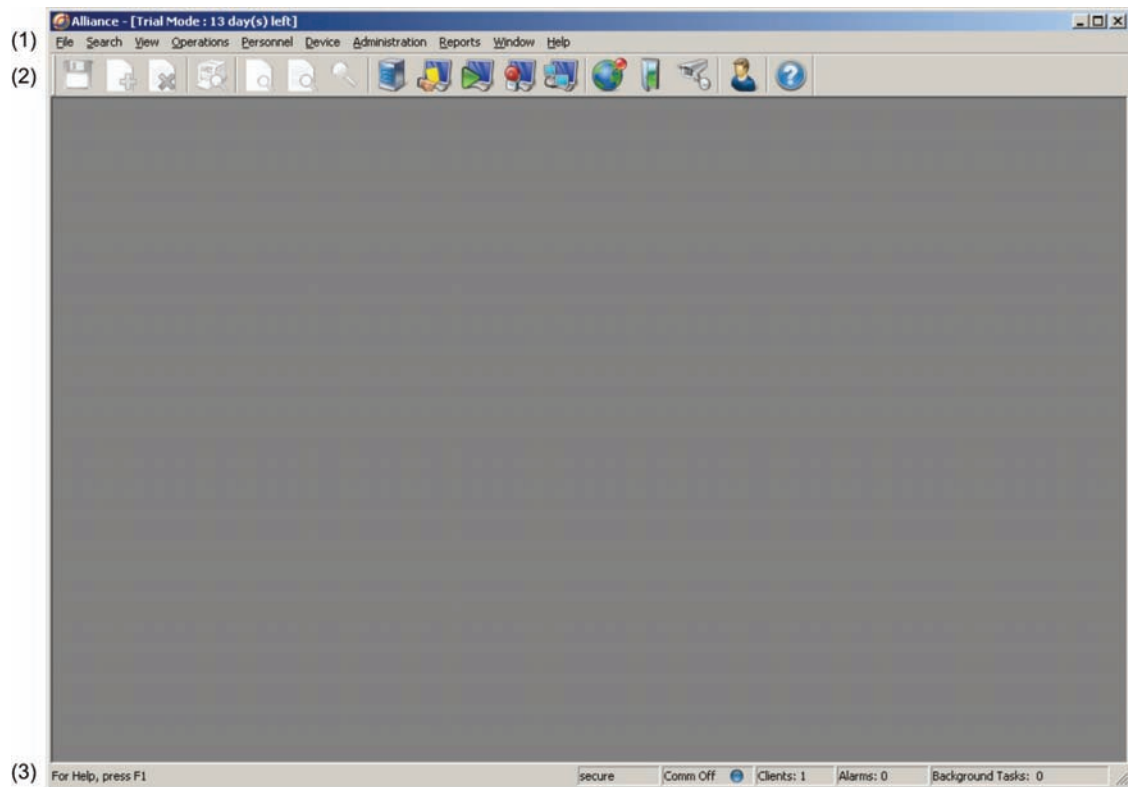
Main window

After starting Alliance 8300 and logging in, the main window displays the following items:

- Menu bar (described in "File Menu" on page 25)
- Toolbar (described in "Toolbar" on page 21)
- Status bar (described in "Status bar" on page 22)

The main window is shown in Figure 6 on page 21.

Figure 6: Alliance 8300 Main Window



- (1) Menu bar
- (2) Toolbar
- (3) Status bar

Toolbar

Toolbar buttons are a quick way to access commonly-used menu items.

Figure 7: Alliance 8300 Main Window Toolbar



From left to right the Toolbar buttons apply the following commands:

- Save button (see “Save Record (Ctrl+S)” on page 25)
- New Record button (see “New Record” on page 25)
- Delete Record button (see “Delete Record” on page 25)
- Print Preview button (see “Print Preview Report” on page 26)
- Clear Search button (see “Clear Search (F7)” on page 27)
- Recall Search button (see “Recall Search (F8)” on page 27)
- Search button (see “Search (F9)” on page 27)
- Controller Utility button (see “Controller Utility (Ctrl+U) [F] [A]” on page 28)

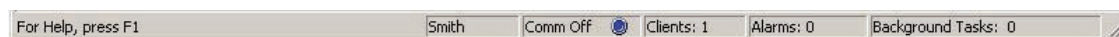
- Badge Monitor button (see “Badge Monitor (Ctrl+B) [A]” on page 28)
- Live History Log button (see “Live History Log [F] [A] [C]” on page 29)
- Alarm Monitor button (see “Alarm Monitor (Ctrl+A) [F] [A] [C]” on page 29)
- Client Monitor button (see “Client Monitor (Ctrl+C)” on page 29)
- Alarm Graphics Viewer button (see “Alarm Graphics Viewer (Ctrl+V)” on page 29)
- Door/Output Control button (see “Door/Output Control (Ctrl+D) [A]” on page 29)
- Digital Video Viewer button (see “Digital Video Viewer [C]” on page 30)
- Person form button (see “Person (Ctrl+P) [A]” on page 31)
- Help button (click the Help button and then click the Alliance 8300 screen to get help).

If you prefer to work without the Alliance 8300 toolbar, in order to provide additional workspace, use the View > Toolbar command to hide the toolbar.

Status bar

The Status Bar option displays the status of the Alliance 8300 system, restricted to the operator’s assigned facilities.

Figure 8: Alliance 8300 Main Window Status Bar



The Alliance 8300 status bar indicates the following:

- For Help, press F1.
- Current operator login ID (the operator in Figure 8 above is ‘Smith’).
- Communication port status.
- Number of clients connected (for the facilities assigned to the current operator, see “Defining facilities” on page 7 for details).
- Number of alarms (for the facilities assigned to the current operator, see “Defining facilities” on page 7 for details).
- Number of background tasks taking place at the Alliance 8300 server computer. If the Status Bar indicates a background task is running, do not shut down the Alliance 8300 services until the task is complete.

If you prefer to work without the Alliance 8300 status bar, in order to provide additional workspace, use the View > Status Bar command to hide the status bar.

Forms

Many Alliance 8300 functions involve the use of forms that have a left-hand side and a right-hand side.

Figure 9: Operator form

The screenshot shows the 'Operator Form' window. On the left, the 'Operator' tab is selected, displaying fields for Login ID, Name, Password, Confirm password, Permission, and Language. The 'Facilities' tab is also visible. On the right, a table displays search results with columns for Login ID, Name, and Language. The table contains one record: 'Secure', 'Default Login', 'English UK'. Below the table, it indicates '(1)' record and 'Records: 1' at the bottom right.

(1) List of records (result of a search).

(2) Details of the selected record.

The right-hand side of the form displays:

- A list of search results.
- The details of a saved record.

Tip: When multiple records are displayed, click a column heading to sort the list by the column. Click a second time to sort in the other direction.

The left-hand side of the form displays:

- Details of the record currently selected in the list of search results.
- Data entry fields for new records.

Using search criteria

The form's data entry fields serve as criteria fields when performing searches. For example, if a facility is selected prior to searching, only the records associated with the facility are searched.

Tab pages

Some forms are used for several types of data entry, which may be grouped into tab pages for ease of use. For example, the Operator form in Figure 9 above has two tabs:

- Operator tab where the operator's details are recorded.
- Facilities tab where particular facilities are assigned to the operator.

Shortcuts

Right click: Alliance 8300 provides right click menus on the left-hand side of most forms (below the tab) for quickly accessing related forms. For example, the Operator form has a right click shortcut to the Permission form.

Figure 10: Example of right click shortcut to Permission form, from the Operator form



Double click: The Controller Setup form, Configuration tab provides double click access to the control panel's devices and configuration settings.

Expand the “+” signs to view the control panel options and devices, and then double click the required item to open the form.

Online Help

Information about forms is provided in a number of ways.

- For general help about the form, press F1 when the form is active to view the online help topic associated with the form.
- For help about a certain part of the form, click the Help toolbar button and then click the item you want help on.
- Some forms have their own toolbars. Hold the cursor over a toolbar button to display the name of the button's command.

Main menu command reference

The Alliance 8300 menu bar provides access to most commands.

This section is a reference to the main menu commands, as described in the Alliance 8300 online help. This section contains only summary information; please refer to the online help for detailed information.

Some menu items have corresponding toolbar buttons — these are indicated below the heading (as applicable). Some menu items have corresponding keyboard shortcuts — these are indicated in brackets in the heading.

Note: For online help when using Alliance 8300, press the F1 button on your keyboard.

File Menu

Save Record (Ctrl+S)



The Save Record command saves changes made to the current record. If you do not save the changes, they will be discarded.

The Save Record command is available:

- When a form that manages records (such as the Badge form) is open in edit mode.
- For operators assigned with permissions of 'update' or 'all' for the selected type of record.
- After a New record is created.

The Save Record button is disabled (greyed) following the Clear Search command, or when there is nothing to save.

New Record



The New Record command creates a new record and enables the Save Record button.

For some record types, the new record is preloaded with default data (except where default data is potentially damaging or confusing).

The New Record command is available:

- When a form that manages records (such as the Badge form) is open
- For operators assigned with permissions of 'update' or 'all' for the selected type of record

Delete Record



The Delete Record command deletes the current record. BE CAREFUL when executing this command, because deleted records cannot be recovered! The Delete Record command is available only when a form is open and contains records, such as the Badge form, and you have been given all permissions.

Some forms do not have a delete command.

Notes

The Notes command opens a text file (notes.txt) in which you can record site-specific information. The program used to edit this file is the program that has

been associated with TXT files in Windows, usually Notepad. Notes.txt is saved to your Alliance 8300 directory.

Logoff (Ctrl+L)

The Logoff command allows you to log off the system without exiting Alliance 8300. While logged off, no one can enter data into Alliance 8300 but it continues to communicate with the control panels, store alarm and badge transactions in the history database, and notify you about alarms. See the Client form for information on turning alarm notifications on and off.

Print Setup

Select File > Print Setup to select your printer, printer properties, paper source, and orientation.

Print Preview Report



The Print Preview Report command allows you to preview a report before printing it. A printer must be added to your computer system in order for this feature to work.

Note: On the Preview Report screen, the Total: field represents the number of records in the database and not the number of records that matched your search criteria. The zoom% value will always read 100% regardless of the zoom used.

Print Report

The Print Report command allows you to send the current report to the currently-selected printer.

Export

The Export command allows you to select an export format for your report. There are a variety of formats available including text, Word for Windows, Lotus, HTML and Excel.

Select an export destination for the report to the application, a file, database, Exchange Folder, or Microsoft Mail (MAPI).

Save Template As

Run this command to save the report template under a new file name.

Set As Default Template

Use this command to select a report template to use as the default template. This template will automatically be loaded whenever you open this report form.

Create Default Template

Use this command to clear the template selection from a report so that a new template can be created from scratch (not based on any other template).

After clearing the Template field on the report form, use the Save Template As... command to name the new template, and then use the Set As Default Template command to make the template the default setting for the report type.

Delete Template

Use this command to clear the current report template

Exit

Exit the Alliance 8300 client application by selecting File > Exit to log out the operator and shut down the Alliance 8300 client application.

Search Menu

Clear Search (F7)



The Clear Search command clears all data in the current form. Use this command when the form has data and you wish to start a new search.

Note that the command does not conduct a search nor does it affect any data in the database. It only clears data from the form in preparation for a search. The Clear Search command is available only when a form that contains records is open, such as the Badge form.

This button can also be used to abort a change to a record.

Recall Search (F8)



The Recall Search command refills the current form with the last search criteria data. Use this command when you wish to recall the last search criteria. The command does not conduct a search or affect any data in the database. The Recall Search command is available only when a form that contains records is open, such as the Badge form.

Search (F9)



The Search command conducts a search in the database for all records that match the search criteria data you enter in the form. The records found by the search are displayed in the search results window. Data can be in any number of fields in the form or any number of tabs. If no data is entered, then all records will be displayed.

Only records that match all fields in which data are entered are displayed.

Asterisks (*) can be placed in text boxes to indicate any characters. For instance, in the Badge form, entering an A* in the Description field will display all badge records that have a description starting with A. Entering *a in the description field will display all badges that have a description ending with a.

If A* is in the Description field and Active is in the Status field, only those badge records with a description starting with A and a status of Active will be displayed. The Search command is available only when a form that contains records is open, such as the Badge form.

View Menu

Toolbar

The Toolbar option determines whether or not the toolbar is visible across the top of your Alliance 8300 screen. This is a toggle selection.

See also “Toolbar” on page 21.

Status Bar

The Status Bar option displays the status of the Alliance 8300 system, restricted to the operator’s assigned facilities. This is a toggle selection.

See also “Status bar” on page 22.

Flat Toolbar

The Flat Toolbar item is not a selectable option and has no relational capability. It is the look of the Alliance display after login.

Split

The Split command allows you to change the horizontal size of the search results window on a form using either the mouse or the keyboard.

Alternatively, left click the vertical separator and drag it to the required position.

Next Pane

The Next Pane command moves the cursor between the main form, the tabs and the search results window, if there is one.

Operations Menu

Controller Utility (Ctrl+U) [F] [A]



The Controller Utility command allows you to monitor communications, control and program the control panel.

Badge Monitor (Ctrl+B) [A]



The Badge Monitor command allows you to monitor badge activity.

Live History Log [F] [A] [C]



The Live History Log command allows you to monitor both alarm and badge activities.

Alarm Monitor (Ctrl+A) [F] [A] [C]



The Alarm Monitor command allows you to monitor alarm activity.

Client Monitor (Ctrl+C)



The Client Monitor command allows you to obtain client information such as client type, Imaging status, and connection status.

Alarm Graphics Editor [F] [A] [C]

The Alarm Graphics Editor command allows you to add icons on graphical map views to point out the location and type of incoming alarms. You cannot create a map using Alliance 8300; create it using the program of your choice and save it in a WMF, EMF, BMP, PG or PNG format.

Alarm Graphics Viewer (Ctrl+V)



The Alarm Graphics Viewer command allows you to view the maps of your facility that were created. These maps point out the location and type of incoming alarms.

Zone Control [A]

See “Zone Control” on page 76 for details about this command.

Zone Status [A]

See “Zone Status” on page 76 for details about this command.

Door/Output Control (Ctrl+D) [A]



The Door/Output Control command allows you to manually open or close doors, or turn on or off outputs.

See “Door/Output Control” on page 77 for details about this command.

Door/Output Status [A]

See “Door/Output Status” on page 77 (Intrusion / Access control) for details about this command.

High Security Regions Control [A]

See “Managing high security regions” on page 78 for details about this command.

Lift Control [A]

See “Lift Control” on page 78 (Access control) for details about this command.

Lift Status [A]

See “Lift Status” on page 78 (Access control) for details about this command.

Area Control [A]

See “Area Control” on page 78 (Intrusion) for details about this command.

Area Status [A]

See “Area Status” on page 79 (Intrusion) for details about this command.

Arming Station Control [A]

See “Arming Station Control” on page 79 (Intrusion / Access control) for details about this command.

Arming Station Status [A]

See “Arming Station Status” on page 79 (Intrusion / Access control) for details about this command.

DGP/Controller Control [A]

See “DGP / Controller Control” on page 79 (Intrusion / Access control) for details about this command.

DGP/Controller Status [A]

See “DGP / Controller Status” on page 80 (Intrusion) for details about this command.

TML Control

See “Managing time locks (TML)” on page 80 for details on time locks control.

FAS Control and Status [F]

The Fire Alarm Systems Control and Status command is described in the *Alliance 8300 FAS Reference Guide*.

Digital Video Viewer [C]



The Digital Video Viewer menu command opens a video command and control application that allows you to monitor digital video multiplexers/recorders and their associated cameras, control live video, as well as search and play back recorded video events.

Change Password

The Change Password command menu opens the Change Password form which allows you to change your password.

Select Facilities

The Select Facilities command opens the Set Active Facilities form which allows you to change the facilities currently in use.

User Walk Test

See “Performing engineer walk test or user walk test” on page 81 for more details on walk tests.

Engineer Walk Test

See “Performing engineer walk test or user walk test” on page 81 for more details on walk tests.

Camera Footage on alarm [C]

Select the Camera Footage on Alarm option to automatically display camera footage on alarm, if a corresponding trigger is defined. The video window will be displayed until an operator will close it manually.

Show map on alarm

If enabled, the map containing the device in alarm (if any) will open automatically.

See also “Alarm Graphics Editor [F] [A] [C]” on page 29.

Personnel Menu

Person (Ctrl+P) [A]



The Person command opens the Person form which allows you to enter a person record into the system. You will enter information such as the name and address, assign access rights for access control, assign a department or user fields and even capture a photo.

Person Profile

The Person Profile defines the set of access rights for a category of person:

- Alarm Groups determine the areas, control panel commands, and control panel menu options can be used by the person profile. There may be no more than one Alarm Group per control panel assigned to a profile.
- Door Groups determine the doors (readers) that can be accessed by the person profile, and within which times. There may be no more than one Door Group per control panel assigned to a profile.

- Floor Groups determine the floors that can be accessed from a lift by the person profile, and within which times. There may be no more than one Floor Group per control panel assigned to a profile.

Personnel Type

The Personnel Type command opens the Personnel Type form which allows you to create groupings of employees. There are three provided with the system: Permanent, Contractor and Temporary. You can also assign a badge design to the personnel type.

Department

The Department command opens the Department form which allows you to create departments which can then be assigned to person records.

Badge

A badge is used to identify persons in the Intrusion / Access control system. Often may have a site code and a badge number. Alternatively badges may be learned by the system without using site code or card numbers.

The Alliance term “Badge” applies to badges and/or a PIN (personal identification number) — a number that is entered on a RAS keypad.

See also “Badges” on page 65.

Badge Groups

Badge groups tell the Alliance 8300 system which badges need to be downloaded to which control panels. Badge groups are linked to control panels via the Controller Setup form, Badge Groups tab.

See also “Badge groups” on page 65.

Badge Design

The Badge Design command opens the Badge Design form which allows you to create a format or design that will print on the badge. See also *Alliance 8300 Imaging User Guide*.

Badge Programmer

The Badge Programmer command launches the external Alliance 8700 Smart Card Programmer application. Alliance 8700, used in conjunction with ATS1620 series Smart Card Programmer hardware may be used to program user badges and reader configuration badges.

Device Menu

The Device menu provides access to forms that control the following categories of devices (listed in the order that they appear in the Device menu):

- All devices associated with an Advisor Master control panel
- CCTV Digital Video Recorders and Cameras

- All devices associated with Fire alarm Systems

Additionally, the Device menu provides an access to the Alarms form.

Alarms

The Alarm command allows you to modify the records that are automatically generated when you define a device.

See also “Configuring alarms” on page 57.

Advisor Master menu options [A]

Advisor Master > Setup

Use the Advisor Master > Setup command to open the Controller Setup form to define or edit the details of a control panel.

Advisor Master > Door Groups

Used to specify when access to specific doors will be granted for a group of persons. Door groups are assigned to person profiles. Each door within the group may have a different time zone when access to the door will be granted.

Advisor Master > Floor Groups

Used to specify when access to specific floors will be granted for a group of persons. Floor groups are assigned to person profiles. Different floors can have different periods (timezones) when access to the floor will be granted.

Advisor Master > Holidays

The Holidays menu allows you to enter 24 (or 64 when using memory expansion) different Holidays for the control panel. The holidays recorded here are used in conjunction with timezones to control access or alarm functions etc., for example, Staff allowed access during normal weekdays can be denied access on weekdays declared a holiday..

Advisor Master > Installer menu options

The Advisor Master Installer menu options are organised in the menu structure in the same order that they appear in a control panel Installer menu, accessed via an LCD RAS (Remote Arming Station).

Note: In the following sections, the text “Installer >” in the heading indicates the menu structure begins with Device > Advisor Master > Installer. Further sub-menu structure is not mimicked here for reasons of brevity.

Under normal circumstances the Advisor Master> Installer section is enabled only for Installers of the Advisor Master control panels.

Installer > Zone Database

Use Zones Setup to program all zone parameters. Each zone is a physical input on the control panel, a DGP or a plug-in zone expander.

Installer > Area Database

The Areas Setup form is used to record information relating to an individual area and can be programmed with a number of options, like the area name, entry and exit times, event flags etc.

Installer > Arming Stations

RASs (Remote Arming Stations) are devices used to provide system control, such as arming or disarming of areas to users. Depending on the type of arming station, additional functions may be available.

Installer > DGP

This DGP menu contains a mixture of data entry fields and check boxes and enables or disables DGPs (Data Gathering Panels). Also the type of DGP can be programmed.

Installer > Alarm Groups

Alarm groups provide the means to control the alarm system (also called alarm control) for Person Profiles, Zones, Doors, and Arming Stations.

Alarm groups have areas, menu options, panel options and timezones.

Alarm groups are assigned to Person Profiles, and to each door/RAS to perform functions. This provides flexibility when determining a person's access to, and control of, the system.

Installer > Timers

The Timer Setup form is slightly different from most other windows, it is a one-off record for each control panel, for example, every Alliance control panel has only one Timer database record. All the fields are data entry fields and have a range of blank (representing zero) or 1 to 255.

Program all system-wide timers in this section.

Installer > System Options > System Options

System options menu is slightly different from most other windows, it is a one-off record for each Alliance, for example, every control panel has only one System options record. This function is used to record options common to the whole system.

Installer > System Options > Custom LCD message

Custom LCD message allows you to modify the text displayed on the RASs connected to the Panel. You may enter up to 32 characters for this text. You will only see this text displayed on the RASs if there are no alarms, system or fault messages.

Installer > System Options > Next Service

Set a date and text to appear for the next routine service call.

Installer > System Options > Auto Reset

This function is used to program the control panel to automatically reset alarms. The reset of alarms are for selected areas (determined by an alarm group) and are reset after a predetermined time that is programmed in this window. Use this facility when it may not always be possible to reset an alarm manually.

Installer > Communications > Computer Connection

The Computer Connection Setup form defines the control panel's setting for communications and reporting.

Communication setting must also be defined for the control panel record in Alliance 8300 via the Controller Setup form, Communications tab.

Installer > Communications > Central Station

This window is used to program all the settings for a specific central station.

Installer > Communications > CS Reporting

This window is used to program all system wide Central Station alarm reporting communication options for PSTN, ISDN, GSM and IP.

Installer > Text Words

This function is one of the ways to add user-defined words to the pre-defined Alliance word library. All words in the library are identified by a reference number. The pre-defined word library uses reference numbers 001 to 899, additional user-defined words use reference numbers from 900 to 999.

Installer > Timezones

Timezones are used to create time slots in which certain events can take place. For example: to automatically arm areas, disable users, or to activate outputs to open a door.

Timezones are assigned to alarm groups, door groups, floor groups, relays/outputs, arm/disarm timers, and Out of Hours Access reporting to restrict/enable some control panel operations during specific time periods.

There are two main types of timezone. These have the same function, except for the following:

- Hard timezones are based on defined times and dates
- Soft timezones are based on events

Installer > Alarm Group Restrictions

Alarm group restrictions restrict alarm groups arming/disarming behaviour. It is an excellent tool to provide additional security options to users.

For example, during the daytime, shops in a shopping mall are not allowed to arm or disarm adjacent shops, but during nighttime they are able to arm and reset.

Installer > Event to Output

The event to output window sets all options to link event flags to outputs.

Installer > Auto arm/disarm

Timezones are used to automatically arm and/or disarm areas. Areas being armed or disarmed automatically do not require any operator action.

Installer > Vault areas

Vault areas, when armed, are areas that will automatically arm other areas after a preset delay time.

By using a special programming procedure, an alarm group restriction timer starts when all of the vault areas are armed. When the timer expires, a non-vault area linked to the vault areas will automatically arm.

Installer > Area Links

In an intruder alarm with multiple areas, the entrance to the premises may be shared by all areas. This shared area should only be armed when the last area is armed. The shared area is known as a common area.

The simplest way to have a common entrance is by assigned multiple areas to a zone. This zone will only generate an alarm if all assigned areas are armed. The longest exit and entry times for the areas will be used.

The other way to create a common area is by using a dedicated area. By linking another area to this common area, the common area will arm automatically when the last (linked) area is armed. As soon as any of the linked areas disarm, the common area will also disarm.

Installer >Zone Shunts

A shunt procedure inhibits an active zone from generating an alarm during a certain time period.

- A zone shunt is initiated when an output is activated, for example, by a door unlocking or by a keypad entry.
- During the shunt time the zone is inhibited.
- If the zone is still active after the shunt time has expired, the zone may generate an alarm, depending on the zone type and the status of the area.
- The shunt timers (16 available) may be programmed individually to control each zone shunt.
- Before the shunt timer expires, a warning may be given.
- A zone shunt stops a door generating an alarm when it's opened.

Installer > TZ to follow output

Select a timezone to follow an output. When the output is active, the timezone is valid, and when restored, invalid. This is reversed if the output is inverted.

Timezones that follow outputs are also referred to as soft time zones. Hard timezones are valid between programmed start and end-times. For example:

- To prohibit the use of a keypad, unless a keyswitch on a zone is active
- To allow an area to be disarmed only if another area is first disarmed

Installer > Printer

Program the details for the printer attached to the control panel.

Installer > Battery Test

This menu contains details regarding the battery test to be run for any batteries on the control panel system databus. All batteries are tested sequentially to prevent power problems. If a battery is disconnected for more than 10 minutes, a warning will be given.

During the battery test, the control panel and/or DGPs, and all auxiliary driven devices, are powered from the battery. Devices are tested one at a time, making sure that not all devices switch to battery test at the same time.

Installer > Event Flag Descriptions

This lists all Event flags programmed in the control panel, along with a description for each.

Installer > System Event Flags

Program the values of system event flags. Valid entries are blank (representing zero) or numbers in the range of 1 to 255.

These event flags are activated when any of the conditions specified exist in the system. Default setting (blank) is No event. The system alarm/fault event flags will be latching if Latching System Alarms is set to YES in System Options.

Note: Take care not to assign Event flag numbers, which are pre-defined (Event Flags 1 to 16), or Event Flag numbers, which have been assigned by the Installer in the Zone Database, Area Database, RAS Database, or Zone Shunts.

Installer > Macro Logic

This function is used to activate an event flag or a zone under specific logic conditions.

Up to four outputs or event flags can be included in the logic equation. Each output or event flag in the logic equation can be programmed as an AND or OR function and can also be programmed to invert the logic. Programming options are provided so that the result of the equation (event flag or zone) will pulse, time, on delay, off delay or latch when true.

Note: It is very important to plan the Macro Logic carefully on paper, noting all details, and the origin of every zone and/or event flags, before attempting to program.

Installer > To remote devices > 4 Door/Lift DGP > General

Use the 4 Door/Lift DGP Setup to program DGPs associated with Intelligent four-door controllers.

Note: You must use the Installer > DGP Setup form to define the Four-Door or Four-Lift DGPs before using this form.

Installer > To remote devices > 4 Door/Lift DGP > Doors

Use Doors Setup to program individual doors associated with Intelligent four-door controllers.

Installer > To remote devices > 4 Door/Lift DGP > Lifts

The Lifts Setup form is used to set up all lift (elevator) options for Intelligent four-lift controllers.

Installer > To remote devices > 4 Door/Lift DGP > Floors

Displays the details for a floor on an Intelligent four-lift controller. This has to be programmed before floor groups can be assigned.

Installer > To remote devices > 4 Door/Lift DGP > Regions

Regions are used by Intelligent four-door/four-lift controllers in combination with anti-passback. Alliance 8300 also uses regions to be able to report on which region users can be found.

Installer > To remote devices > 4 Door/Lift DGP > DGP Macro Logic

Macro logic provides a powerful tool for activating event flags when specific events occur. These events are macro inputs being triggered, logic equations combining the macro inputs, and timed/latched output conditions.

Up to four macro inputs may be included in the logic equation. A macro input is an event flag. Each macro input in the logic equation can be programmed as an AND or an OR function and may be inverted.

Options are provided so that the macros result will trigger a macro output, which may be: a pulse, timed, on delay, off delay or latched when activated.

Installer > To remote devices > 4 Door/Lift DGP > DGP Card Batches

Card batches are used to provide easier programming of a range of consecutive cards into the Intelligent four-door/four-lift DGP, while also allowing for multiple system codes.

Each of the 40 available card batches provides:

- A system code
- A number of cards
- A starting user number

Installer > To remote devices > IADS DGP > General

Use IADS DGP Setup to program the mode and protocol for a particular IADS (intelligent addressable device system) DGP.

Note: You must use the Installer > DGP Setup form to define an IADS DGP before using this form.

Installer > To remote devices > IADS DGP > Devices

Use IADS DGP Devices Setup to program the address, type, and other defining parameters for individual IADS DGP devices.

Installer > To remote devices > Wireless DGP > General

Use Wireless DGP Setup to program the mode and other options for a particular Wireless DGP.

Note: You must use the Installer > DGP Setup form to define a Wireless DGP before using this form.

Installer > To remote devices > Wireless DGP > Zones

Use Wireless DGP Zone Sensors Setup to program the label code, zone data, and other defining parameters for individual Wireless DGP zone sensors.

Installer > To remote devices > Wireless DGP > Fobs

Use Wireless DGP Fob Sensors Setup to program the label code, button assignment, and other defining parameters for individual Wireless DGP fob sensors.

Installer > To remote devices > Advanced DGP

Use Advanced DGP Setup form to program the mode and the following options for a particular Advanced DGP:

- Battery load enabled
- Clocked output enabled
- Mains Check enabled

Note: You must use the Installer > DGP Setup form to define an advanced DGP before using this form.

Installer > To remote devices > Bank DGP> General

Use Bank DGP Setup form to program the mode and other options for a particular bank DGP.

Note: You must use the Installer > DGP Setup form to define a bank DGP before using this form.

Installer > To remote devices > Bank DGP > TML Groups

Use TML Group form to program time locks group mode, TML assignments, area and time zone, as well as some options for the selected group as reporting and logging of various events.

Installer > To remote devices > Bank DGP > RAS Options

Use RAS Options form to program the options for RASes connected to the bank DGP. These options include areas and alarm group assignment, alarm options and other reader and keypad options.

Installer > To remote devices > Bank DGP > Card Batches

Card batches for bank DGP are defined as for four-door controller. See “Installer > To remote devices > 4 Door/Lift DGP > DGP Card Batches” on page 38.

Installer > Clock Correction

This command allows a correction factor to be programmed into the control panel to compensate for a control panel clock that may be running slightly fast or slow.

Installer > Class Database

Reporting of alarms depends on the settings in Reporting code in the Zone database. This setting is a reporting class. There are 8 classes containing 6 conditions that can be selected for reporting.

The order of programming after selecting the control panel is:

- Select the class (medical, fire etc.)
- Select the reporting condition (inhibit, uninhibited, etc.)
- Enable or disable the reporting by selecting or deselecting the central station number

Installer > Test Calls

This menu holds all programming concerning test call reporting.

Installer > System event to channel map

This is the 200 Baud FSK French communication command.

Installer > Voice Reporting

Use this command to assign a voice message number from the Voice Module (for example, ATS7200) to specified event numbers.

Installer > DVMR Configuration (via RS232)

Use this command to configure an 8-area or a 16-area control panel for connection to a DVMR (Digital Video Multiplexer Recorder) via a Serial Computer and Printer Interface printer port installed on the control panel.

The serial computer and printer interface must be connected to the RS232/1 port on the DVMR. This connection is referred to as a high-level interface (HLI).

The HLI enables security staff to operate the DVMR via permitted RAS keypads to search for and view recorded video.

Refer to the appropriate control panel programming manual for detailed instructions.

CCTV menu options [C]

CCTV > Digital Video Device

The Digital Video Device menu item opens the Digital Video Device form that allows you to define, configure, and request status of your digital video devices.

CCTV > Camera

The Camera form menu item of the Device menu opens the Camera form, allowing you to edit your camera database records.

FAS Menu Options [F]

FAS > Setup

These options allow to configure options necessary to interface to the Fire Alarm System equipment. Please refer to the *Alliance 8300 FAS Reference Guide*.

FAS > Devices

Use the Devices command to change description and state icons for supported Fire Alarm System point types. You can change the default icon for each state a point type may have.

Administration Menu

Operator

The Operator command opens the Operator form that allows you to set up individuals as users for the Alliance 8300 system and assign the facilities to which they have access.

Permission

The Permission command opens the Permission form that allows you to define Operator access to various forms within Alliance 8300.

Client

The Client command opens the Client form allowing you to define a client computer.

API Connections

The API Connections command opens the API Connections form that allows you to define records to enable external applications to interface with Alliance 8300. See also the *Alliance 8300 API Manual*.

Instruction

The Instruction command opens the Alarm Instructions form that allows you to create instructions to link with alarms. The instruction(s) will then appear on the Alarm Monitor when the alarm occurs.

Response/Purpose

The Response/Purpose command opens the Response/Purpose form that allows you to create a predefined response to an alarm or a purpose for a control option. These responses/purposes are used in the Alarm Monitor or any control command in the Operations menu.

Parameters

The Parameters command opens the Parameters form that allows you to establish settings for the entire application, such as archive intervals and appropriate modems.

Override

The Override command opens the Override form that allows an operator to generate a T/A (time in attendance) transaction. This information is written to history.

LogFile

The LogFile command opens the Logfile form. The LogFile form allows you to select your computer and name the LogFile, and enter the path and directory in which to place your logfile.

Diagnostic Setting

The Diagnostic Setting command opens the Diagnostic Setting form that allows you to define what debug information will go to the diagnostics log. This is a good place to start for troubleshooting.

Note: Apply these settings only on request of appropriate Support personnel to avoid logging unnecessary data in the diagnostic logs.

Diagnostic Viewer

The Diagnostic Viewer command allows you to view what's happening on the system. The debug messages displayed by the DiagView program are determined by the items you select in the Diagnostic Setting form.

CCTV Alarm

The CCTV Alarm command opens the CCTV Alarm form that allows you to link a CCTV Interface and alarm to Alliance 8300 so that the CCTV alarms will display on the Alliance 8300 Alarm Monitor.

Note: This feature is currently not supported.

Camera Preset

When you select Camera Preset from the Administration menu, the Camera Preset form displays, allowing you to define PTZ camera presets to select from.

Event Trigger

Event Trigger allows you to move up to four PTZ (pan tilt zoom) cameras into preset positions in response to specific door/reader transactions and/or alarm transactions.

Alarm Category

Alarm categories are used in the Alarm form and the Alarm History Report to provide a means of filtering large numbers of alarms. Use the Alarm Category Setup form to create new alarm categories.

Alarm Notifier

Alarm notifier allows to define alarm notification for particular events. The e-mail settings are configured in the Parameter form. See *Alliance 8300 Online Help* for more details on the e-mail notification parameters.

Facility

The Facility command opens the Facility form that allows you to define the desired facility, such as Building One and Building Two.

Map Background Editor

This form is necessary to setup the application used for editing images that are used as map background.

Point Type Icons

Use the Point Type Icons command to setup description and state icons for supported Advisor Master point types. You can change the default icon for each state a point type may have.

Reports Menu

Refer to “Reports and templates” on page 84 for additional details about reports.

Person

The Person Report command opens the Person Report form that allows you to create a report on the persons in the database. Reports may include personal information, such as address, department, badge, access rights, and user fields on all or a subset of persons in the system.

Badge

The Badge Report command opens the Badge Report form that allows you to create a report on the badges in the system.

Persons in Regions

The Persons in Regions Report command allows you to create a report on the persons that currently are in particular regions.

Administration

The Administration Report command opens the Administration Report form that allows you to create a report on the administrative aspects of the program. Report types include alarm instruction, archive, client, facility, host parameter, operators, permission, and response.

Advisor Master

Generates reports about the Advisor Master control panel devices in the system.

Floor Access

The Floor Access Report command opens the Floor Access Report that allows you to create a report on the floors defined in the system and the access granted to each one.

Door Access

The Door Access Report command opens the Door/RAS Access Report form that allows you to create a report on the persons in the system who have access to any of the specified doors or readers.

Area Access

This command opens the Area Access Report form that allows you to create a report on the persons in the system who have access to any of the specified areas.

Advisor Master Groups

Generates reports about the Door Groups or Floor Groups in the system, for a selected control panel or for all control panels.

Roll Call

The Roll Call Report command opens the Roll Call Report form that allows you to create a report on the people who last entered one of the specified readers. The report provides a list of the last access granted to any or all persons in the system and each of their badges; that is, who last went where.

FAS Devices

This command generates reports about the Fire Alarm System devices in the system. Please refer to *Alliance 8300 FAS Reference Guide* for more details.

Alarm History

The Alarm History Report command opens the Alarm History Report form that allows you to create a report on the history of alarm activity.

Badge History

The Badge History Report command opens the Badge History Report form that allows you to create a report on the history of badge activity.

Time and Attendance History

The Time and Attendance History Report command opens the Time and Attendance History Report form that allows you to create a report on the history of time and attendance activity.

Operator History

The Operator History Report command opens the Operator History Report form that allows you to create a report on the history of operator activity.

External Reports

The External Reports command opens the Launch External Reports window, allowing you to access an executable program or report that was not created within Alliance 8300. Navigate to the program or folder, select the file, and click Open.

Window Menu

Cascade

This command allows you to control multiple windows or forms. If you have several forms open but not visible, use this command for a cascading view of your forms with the active form taking precedence on the display screen.

Tile

This command allows you to control multiple windows or forms. If you have several forms open but not visible, use this command to view all forms tiled side-by-side on your display screen.

Arrange Icons

This command allows you to control multiple windows or forms. If you have several forms in progress, you can temporarily minimize a form from view. Use this command to arrange the minimized form icons across the bottom of your Alliance 8300 window.

Help Menu

Help Topics (F1)

Select Help Topics to launch the Alliance 8300 Online Help.

About Alliance

This screen displays the software version, service pack number, copyright information, and contact information.

Setting system parameters

The Parameters form will be one of the first parts of Alliance 8300 you need to use. For example,

- Before you define a control panel and connect to it, you might want to be set up to print alarm activity.
- Before you add any photos to Person records, you need to ensure that the photo aspect ratio is set correctly.

Note: For the changes on the Parameters form to take effect, you *must* save the change and then stop and restart the Alliance 8300 services. The easiest way to do this is to restart the computer.

System-wide (global) settings for Alliance 8300 are specified on the Parameters form, including:

- The database archive settings (daily, weekly, or monthly)
- Whether to print badge and alarm activity and to which printer(s)
- Alarm sound settings
- Photo aspect ratio for capturing images
- The names of the labels that will be used globally for the user fields and address fields
- Identification of modems that are used to communicate with control panels

The Parameters form is divided into six tab pages:

- Settings tab (see “Settings tab” below).
- User Fields tab (see “User Fields tab” on page 49).
- Address Fields tab (see “Address Fields tab” on page 49).
- Communication Settings tab (see “Communication Settings tab” on page 49).
- Clear Archive tab (see “Clear Archive tab” on page 50).
- Badge Learn tab (see “Badge Learn tab” on page 51).

Settings tab

Archive Database

In the Archive Database section (see Figure 11 on page 47), select to archive history on a daily, weekly, or monthly basis. You can also archive it immediately by pressing Archive Now button.

Figure 11: Parameter form, Settings tab

The screenshot shows the 'Parameter Form' window with the 'Settings' tab selected. The window is divided into several sections for configuring system parameters. The 'Archive Database' section allows selecting the time interval to archive history (Daily, Weekly, or Monthly) and a specific day of the week (Sunday). The 'Alarm activity printing' and 'Badge activity printing' sections each have an 'Enable' checkbox and a 'Select Printer...' button. The 'Console alarm sound' section has radio buttons for 'Continuous' and 'Short'. The 'Photo Aspect Ratio' section has spinners for 'Height' and 'Width'. The 'Alarm Notifier E-mail Support' section includes an 'Enable' checkbox, fields for 'SMTP E-mail Server', 'From E-mail Address', 'To E-mail Address Field', 'E-mail User Name', 'E-mail Password', and 'Confirm Password', along with a 'Send Test E-mail' button.

Note: The default setting is to archive history on a daily basis. It is recommended that you use the default setting. Whatever setting you choose, you must monitor the size of the Alliance 8300 history and archive databases to ensure that each database remains under 2 GB and that the databases do not completely fill the hard disk.

If you select:

- Daily (default setting): The archive is created every day some time between midnight and 1A.M.
- Weekly: The archive is created every week on the day you select sometime between midnight and 1A.M.
- Monthly: The archive is created on the first day of the month some time between midnight and 1A.M.

Archive now

Press this button to archive the history immediately.

Note: If you selected Weekly, there must be at least seven days following the installation date to first archive. For example, if a system was installed on Tuesday and the archive is scheduled for Sunday, the archive will not take place on the first Sunday after installation. Archiving will begin on the second Sunday following the installation.

The Archive Database setting assumes that the Alliance 8300 server is running. If it isn't, then the next time Alliance 8300 is started and a transaction is received, the archive is created.

Alarm Activity Printing

You must enable and select a printer and route alarms to print in order for alarm activity to print.

Console alarm sound

Select Continuous to sound a continuous tone on alarm until the alarm is acknowledged. Alternatively, select Short to sound a short tone when alarms are detected. Sounds for alarms have to be set up separately if needed.

Badge activity printing

You must enable and select a printer and route badges to print in order for badge activity to print.

Photo Aspect Ratio

Enter a number for the height and the width. The aspect ratio controls the relationship between the height and width of the photos. This setting controls the photos displayed in the Capture program, on the Person form, and in the Badge Designer program.

Alarm Notifier E-mail Support

Sets up the e-mail settings for the alarm notifier (defined in the Administration > Alarm Notifier menu). The following options are available:

- To E-mail Address Field: Select the user field, which will be used as an e-mail address of the notification recipients.
- SMTP E-mail Server: The SMTP E-mail sending address.
- From E-mail Address: The e-mail address shown in the "From" field of the e-mail message.
- Allow Anonymous Address: Select this option if the above SMTP server does not require an authorization. Otherwise the settings below are necessary to configure.
- E-mail User Name: The login of the SMTP server account.
- E-mail password, Confirm Password: The password for the SMTP server account.

Click Send Test E-mail to send test e-mail to the address defined in "From E-mail Address".

User Fields tab

User Fields Labels

Displays the current labels for the 90 user fields on the Person form. Select a label to change it.

New label

To change the label of a user field, highlight the desired user field and type the new label. The user field label can be up to 32 characters long.

Address Fields tab

Displays the current labels for the 5 address fields on the Person form. To change a label, type over the existing text. The address field label can be up to 32 characters in length.

Communication Settings tab

Use this tab of the Parameter form to allocate the client modem pool: modems to be used by client computers for communicating with dial-up control panels.

Note: Any change in this section requires Alliance services to be restarted.

Clients list

Select a client computer in the Clients list.

Available modems

Available modems lists all the registered modems for the selected client computer. Click to select one or more modems to enable them to be used by Alliance 8300 (running on the selected client) to connect to a control panel.

Modems reserved for incoming calls

Click the Modems reserved for incoming calls arrows to specify the number of modems you want to reserve on the selected client computer.

Note: The number of modems selected in the Available modems list must be greater than the number of reserved modems in order to make outgoing calls.

Disconnect after idle

Click the Disconnect after idle arrows to select the number of minutes you wish the system to wait before disconnecting from the control panel when the connection is idle (there is no history or database information being exchanged or control/status commands issued).

If you select 0, the connection will not be automatically disconnected by Alliance 8300 when idle.

Clear Archive tab

The Clear Archive tab is depicted in Figure 12 below.

Figure 12: Parameter form, Clear Archive tab

The screenshot shows the 'Parameter Form' window with the 'Clear Archive' tab selected. The window contains the following elements:

- Navigation tabs: Settings, User Fields, Address Fields, Communication Settings, **Clear Archive**, Badge learn.
- Fields: 'Earliest Date in Current Archive DB:' and 'Latest Date in Current Archive DB:'.
- Button: 'Show date'.
- Section: 'Archive clean period'.
- Calendars: Two side-by-side calendar views for January 2011. The first calendar shows dates 26 through 31, with the 21st highlighted. The second calendar shows dates 2 through 5, with the 21st highlighted.
- Date pickers: Two date pickers below the calendars, both showing '2011-01-21'.
- Labels: 'Start Date' and 'End Date' below the date pickers.
- Button: 'Delete' at the bottom center.

Earliest Date in Current Archive DB

This shows the oldest date for an event stored in the Archive database.

Latest Date in Current Archive DB

This shows the most recent date for an event stored in the Archive database.

Show date

If you have an archive database, click Show Date and the Earliest Date in Current Archive DB and Latest Date in Current Archive DB will display. If you do not have an archive database, the two date fields will state No Record.

Archive Clean Period

Select the Start Date of the data that you want to remove from your database by selecting the month, then the day to begin your archive.

Select the End Date of the data that you want to remove from your database by selecting the month, then the day to end your archive.

Delete

Press Delete after selecting Start Date and End Date to remove from your database.

Note: The deletion of an archive database is taking place in the background. Progress is indicated on the status bar. This may take hours to complete and is dependent on the size of the Archive database and the hardware components of your computer.

Badge Learn tab

The Badge Learn tab is used to specify badge learn devices (one, several, or all RASs or doors where badge readers are used). A badge learn device is used to quickly enter raw badge data into Alliance.

Restrict

Select Restrict to prevent all RASs and doors (available to the operator) from being used as badge learn devices on the LAN. When Restrict is selected (default setting), the Edit button is enabled.

Edit

Use the Edit button to add badge learn devices (RASs or doors) to the Badge Learn Devices window. Only the listed badge learn devices may be used to enter raw badge data into Alliance (as long as Restrict is selected).

Permissions, facilities, and operators

Before individuals can access, use, or administer the Alliance 8300 program, they must be set up as operators. The setup sequence is as follows:

- Alliance 8300 permissions and facilities must be created before operators.
- When operators are set up, they must have permissions and one or more facilities assigned.
- At any given time, an operator can choose which facilities to be active from the list of facilities available to that operator.

Note: Operators using an Alliance 8300 client computer and working over a network connection (via either a domain or a workgroup) must be logged into the client computer's operating system using a login ID and password combination that provides appropriate access permissions to the shared folders on the Alliance 8300 server computer. Alliance 8300 installation DOES NOT create any users or permissions under the domain environment.

Creating Alliance 8300 permissions

Permissions are assigned to operators and define what operators can do within Alliance 8300. Use the Permission form to create permission records.

For example, if a Personnel Officer needs to use the Personnel menu, certain reports, and the Change Password command, you can define a permission that provides access to these functions and no others (other menu options would be greyed the next time the operator logs in).

To locate and view existing records, press the Search button. A list of records will display. You may either press the Add button to add a new record OR search and view or change an existing record.

Alliance 8300 comes with a System Administrator permission that allows full action on all forms and is assigned to the default operator. Additional permissions are:

- Super User (no installer options)
- Installer (restricted personnel options)
- Security (possible permissions for security guards)
- Reception (possible permissions for reception desks)

Any of the available permissions may be changed. You may wish to create more restrictive permissions. Apply the System Administrator permission ONLY to those operators fully trained in Alliance 8300.

Permission form

The Forms list on the Permission form displays the form permissions for the selected Permission record. The list can be viewed in two modes:

- **Show by Group:** Lists the menu groups (File, Operations, Device, Administration, Reports) followed by the menu items in each group. The permission assigned to each group and item is indicated by an action icon.
- **Show by Action:** Lists the actions (none, read, update, all) followed by the forms assigned to each action.

Right click the Forms list to select the required view, or to open the Operator form, which shows permissions assigned to existing operators.

The Forms list displays the forms within the Alliance 8300 program organised by their menu structure. A “+” sign on the left side indicates hidden submenus. You may apply an action to the entire menu, or you can click the “+” to display submenus to apply a mix of actions within the sub-menus.

Four types of actions can be assigned to forms:

- **None:** Means that no access is given to that form.
- **Read:** Means that read only access is given. The form and the associated records can be viewed but not modified.
- **Update:** Means that the records on that form can be viewed and modified.
- **All:** Means that the records on that form can be viewed, modified and deleted.

Mixed is not an action to be assigned. It is used only on this form to signal that any forms beneath a group have different actions assigned.

Adding a permission

Add a new permission record to Alliance 8300.

To add a permission in Alliance 8300:

1. Select Administration > Permission.
2. Select File > New Record. The Permission form displays in edit mode (the Save Record command is enabled).
3. Type a name to describe the new permission in the Description field.
4. Click the “+” beside each form category to display the list of forms. Initially, all forms have the action “None” assigned (no permissions).
5. Select a form and then select the required action (if you need to change the action from None). Repeat for each form name.
6. Save the Permission form.

Creating facilities

The Alliance 8300 database can be partitioned and related records can be grouped. In Alliance 8300, these groups are called facilities. A Facility option can be designated on most forms throughout the system and any number of facilities can be defined. Using facilities will result in showing only those records in a form that have no facility assigned, or are part of the active facilities for an operator.

Note: It is recommended to create facilities and associate new control panels to facilities from the very start (assign a facility to a control panel record before saving the record). This will help ensure that all the data related to the control panel is kept within the same database partition and will help speed access to data.

Operators can be assigned to one or more facilities and can choose which facilities to be active at any given time. Usually, the system administrator is assigned to all facilities.

All records have the default Ignore Facilities, which means the records are not under facility protection; therefore, those records are visible to all operators.

Creating and using facilities are separate things:

- To create a facility, use the Facility form.
- To assign a facility to the required operator, use the Facilities tab on the Operator form.
- To manage a facility's state, use the Select Facilities command from the Operations menu.

Note: If you, as an operator, do not have a particular facility assigned to you, that facility will not be available to you from the Facilities list on various forms.

Adding a facility

To add a facility in Alliance 8300:

1. Select Administration > Facility.
2. Select File > New Record. The Facility form displays in edit mode (the Save Record command is enabled).
3. Type a name to describe the new facility in the Description field.
4. Save the Facility form.

Creating operators

An operator is an individual who can access and control the Alliance 8300 software.

An Alliance 8300 operator has a login ID and password for Alliance 8300. This login ID and password is independent of the operator's Windows user account login ID and password.

Note: An Alliance 8300 operator must have a Windows user account before they can use the Alliance 8300 system. An identical Windows user account (with membership to the appropriate groups) must be created on every Alliance 8300 computer in the system (the server and all of the clients). This enables the Alliance 8300 server and client computers to communicate as a workgroup (regardless of whether an Alliance 8300 operator is logged in).

Refer to “Adding Windows users” on page 126 for details of adding Windows user accounts.

Adding an operator

When using the Operator form for search for existing records, use the Ignore Facilities selection to display all operator records. Alternatively, search using a specific facility to locate operators assigned to a particular facility (but not the facilities assigned to an operator).

The Operator form is used to:

- Assign the operator to a facility.
- Define an operator’s login ID, name, and password.
- Assign Permission to an operator. Permissions define the actions that operators may perform within Alliance 8300. Click the Operator tab and then click the Permission arrow to select permission from the list. Permissions are created on the Permission form.

Note: To reduce operator’s permissions, be sure to block access to Permission and Operator menus.

- Assign facilities to operator. Once assigned, the facility is added to the Facility list on various forms when that operator is logged in. Click the Facilities tab to assign a facility to a selected operator. Facilities are created on the Facility form.

To add an operator in Alliance 8300:

1. Select Administration > Operator.
2. Select File > New Record. The Operator form displays in edit mode (the Save Record command is enabled).
3. Type the operator’s login ID (the name that the operator will use to log in to Alliance 8300).
4. Type the operator’s name.
5. Type the operator’s initial password (the operator can change this later using the Operations > Change Password command). The password field displays each character as *.
6. Click the Permission arrow and select the operator’s permission from the list of the available permissions.
7. Click the Language arrow and select the operator’s language.

8. Define if the operator has the option to enter a purpose for issuing a control command in maps, or from the control options in the Operations menu.
9. Click the Facilities tab, and then click the Assign Facilities button to display the Facility Assignment dialog. This dialog lists the facilities available for assignment to this particular operator.
10. Assign the required facilities to the operator.
11. Save the Operator form.

Managing facilities

Facilities assigned to an operator are active by default.

A facility may be set to 'Available' (inactive) when it's not needed. For example, a facility may be created for future use and then made inactive to prevent the facility from being accidentally selected by the operator when using various forms.

Configuring devices

The Alliance 8300 Device menu provides access to forms for configuring:

- Alarms (see “Configuring alarms” below).
- Control panels (see “Advisor Master > Setup” on page 33). See also “Configuring a control panel” on page 58.
- Door groups (see “Advisor Master > Door Groups” on page 33).
- Floor groups (see “Advisor Master > Floor Groups” on page 33).
- Holidays (see “Advisor Master > Holidays” on page 33).
- Advisor Master Installer menu options (see “Advisor Master > Installer menu options” on page 33).
- Digital Video Recorders (see “CCTV > Digital Video Device” on page 41).
- Cameras (see “CCTV > Camera” on page 41).
- Point Types (see “Point Type Icons” on page 43).
- FAS (refer to the *Alliance 8300 FAS Reference Guide*).

Refer to the *Alliance 8300 Online Help* for more details about these options.

Configuring alarms

Alarm records are automatically created by Alliance 8300 when various device records are created. For example, when a Digital Video Recorder record is created using the Device > Digital Video Recorder form and is given a description “Second DVR”, Alliance 8300 automatically creates alarm records for the DVR with the following attributes:

- The Description field displays the alarm description, for example, “DVR Disk Full Alarm”.
- The Facility field displays the facility that Digital Video Recorder record was assigned to.
- The Owner Description field displays “Second DVR”, which is the content of the description field for the Digital Video Recorder record.
- The Owner Type field displays “UTC F&S DVMR”, which identifies the alarm owner (such as a control panel or DVR) by the generic type of device.
- The Category field displays the alarm category, such as “CCTV Alarm”.
- The Monitor field displays if the alarm should be shown in the Alarm Monitor.

When first opened, the Alarm form displays in Search Mode. The New Record command is not an option for this form because Alarm records are generated by the system. The Save command becomes active only when alarms are displayed in the list on the right-hand side of the window (see page “Forms” on page 23).

The total number of alarms can become quite large; therefore it’s useful to filter the search.

For example, to display only the alarms from a particular facility:

1. Run the Search > Clear Search command to clear the form of data.
2. Click the Facility arrow and select the required facility from the list. (The facility must be both active and assigned to you as an operator.)
3. Run the Search > Search command to display all alarm records that have been created for the facility.

In the same manner, other fields can be used to filter the search. Refer to the *Alliance 8300 Online Help* for further details.

After selecting the required alarm on the right-hand side of the window, edit the details as required on the Alarm, Instruction, or CCTV tabs, and then save the alarm record.

Configuring a control panel

Note: Before saving a new record for a control panel with existing users, remove the MASTER badge groups to avoid overwriting users 1 and 50 in the control panel.

The process of setting up a control panel in Alliance 8300 is simplified when the control panel has previously been set up. In this case, all that's required is to define the control panel record in Alliance 8300, connect to the panel, set it online, and upload (retrieve) the panel's database for editing in Alliance 8300.

The uploaded database populates or updates the default values in the Alliance 8300 database, except for:

- User records
- Facility assignment
- Device descriptions

This process is described in the *Alliance 8300 Installation Manual*.

In cases where a new control panel is being set up, it is useful to know the most efficient sequence for programming and where in Alliance 8300 various steps are performed.

The following sections describe recommended basic and advanced set-up sequences for initially programming a control panel.

Standard alarm system programming

Using the recommended programming order provides the most efficient programming and makes sure that no item is forgotten when setting up a system. It is assumed that the control panel and all required devices are connected and the database has been uploaded.

Note: When using four-door, four-lift or wireless controllers, enable polling first, set the appropriate DGP type, and only then upload the database to retrieve information of these devices.

All options can be accessed via the Device > Advisor Master > Setup menu (Configuration tab), except where indicated otherwise.

To program the system:

1. Gather all information like maps, where detectors are located, what areas are available, etc.
2. Set up Alliance 8300 and the control panel to communicate. This process is described in the Alliance 8300 Installation Manual.
3. Program control panel system options.
4. Program all names that are not in the standard word library using text words. (Alliance 8300 recognises when new words are used and offers to create new text words automatically.)
5. Program all required timezones.
6. Program area details.
7. Program all required alarm groups.
8. Program/activate all connected RASs (arming stations).
9. Program/activate all connected DGPs.
10. Program all available or required zones.
11. Program all required communication settings and central stations for alarm reporting.
12. Set all reporting related issues in the class database.
13. In the Report Test command, program test call details.
14. Map events to outputs. Take care all event flags have a clear description.
15. Program required Access Rights, Persons, and Badges. This process is described in "Access rights, persons, and badges" on page 64.

Additional alarm system programming

When the standard set-up has been taken care of, additional options might be required. Following is a list of options, all of which can be accessed via the Device > Advisor Master > Setup menu (Configuration tab).

- If common building entry is required for alarm control, assign more than one area to a zone, or use Area linking.
- For special access (for example, cleaners) an alarm groups may require restricted options.
- When timed disarm is selected in alarm group restriction, program the disarmed period.
- Program automatic arming/disarming.
- Program required system options.
- Program extensive battery testing (if required).

- Program printer settings if a printer is to be connected.
- Configure timezones that are activated by outputs.
- Program required macro logic.
- Enter the required custom message for LCD RASs.
- Program automatic reset of areas.
- Program any areas required to be vault areas.
- Program zone shunts.
- Enter the next service date details.
- Program standard access control using RASs 1 through 16 (see next section).
- Program a relay control group to each RAS (door).
- Program any required door groups (see next section).

Using a four-door/lift DGP in access control system programming

Using the recommended programming order for an access control system ensures efficient programming and that no item is forgotten while programming the Advisor Master four-door/four-lift DGP (four-door/lift DGP).

All options can be accessed via the Device > Advisor Master > Installer > To remote Devices > 4 Door/Lift DGP menu, except where indicated otherwise.

Standard four-door/lift DGP programming

To program a four-door/lift DGP:

1. On the Advisor Master DGP Setup form, set the DGP address for the four-door DGP (see Numbering in the Alliance 8300 Online Help).
2. Set addresses of RASs (readers or DGPs connected to the local databus of the four-door/four-lift DGP (see Numbering in the Alliance 8300 Online Help).
3. Activate polling for the four-door/four-lift DGP and set the DGP type.
4. Upload the panel data to retrieve the default configuration.
5. Check in system options the dual zone setting and the number of prefix digits.
6. Program timezones required for access control functions (Request to Exit Options, Override Timezone, and Door Groups).
7. Determine which area(s) will inhibit Request to Exit or Access through a door when the area/s are armed.
8. On the Advisor Master four-door/four-lift DGP Setup form, program four-door/Lift DGP options:
 - Output controllers

- Card batches (on the DGP Card batches form)
 - Alarm code prefix digits
 - Poll RASs (on local databus)
 - List RASs with LCD display
 - List RASs with Request To Exit input enabled
 - Poll DGPs (on local databus)
 - Set Tamper monitoring (dual zone) option
 - Enter Card to PIN time
 - Enter Two card time
 - Enter Multi-badge time
 - Enter re-lock delay time
 - Enter region count limit
9. On the Advisor Master doors setup form (Access options tab), program the following:
- Enter the door to program
 - Enter the unlock time
 - Enter the extended unlock time (if required)
 - Select the shunt option (if required)
 - Enter the shunt time (if required)
 - Enter the extended shunt time (if required)
 - Enter the shunt warning time (if required)
 - Enter the low security timezone (if required)
 - Select if the IN or OUT reader requires Badge & PIN
 - Select if PIN is required during timezone
 - Select if Anti-Passback is required
 - Enter the IN & OUT reader region (if required)
 - Select if IN or OUT reader requires Two card function
10. On the Advisor Master doors setup form (Request To Exit options tab), program the following (if required):
- Enter the Request To Exit timezone
 - Select the Request To Exit option
 - Select if IN or OUT Request To Exit should be disabled when armed
 - Select if Request To Exit should be reported
11. On the Advisor Master doors setup form (Reader options tab), program the following:
- Select the card format used
 - Select the override timezone (if required)
 - Select the LED function (if required)
 - Select if the door zone should keep the door unlocked
 - Select if the unlock timezone should only start after entry
 - Select if the door open/close should be reported
 - Select if forced opening is to be reported
 - Select if the door should be held unlocked until the door opens
 - Select if the door closed and locked is reported as locked
 - Select if Door Open Too Long has to be reported
 - Select if the reader is a Time and Attendance reader.

- Select if a pulsed lock/unlock is required
 - Select if duress is to be disabled
 - Select if closed and locked is to be reported as locked
12. On the Advisor Master doors setup form (Hardware options tab), program the following:
- Enter the unlock output number
 - Enter the forced output number (if required)
 - Enter the warning output number (if required)
 - Enter the Door Open Too Long zone number (if required)
 - Enter the Door Open Too Long output number (if required)
 - Enter the Request To Exit zone number (if required)
 - Enter the fault output number (if required)
 - Enter the (door) zone number
 - Select if the 2nd door zone should be monitored
 - Select the shunt zones (if required)
 - Select the interlock zones (if required)
 - Select the area/s assigned to the door (if required)
13. On the Advisor Master door groups setup form, program the required door groups.
14. On the Person profile setup form program the Person profiles that require access control functions (door groups).
15. Program zones available on the four-door DGP.

Additional four-door/lift DGP programming

Alarm control

Use the following steps to program alarm control functions.

To program alarm control:

1. Program timezones required for alarm control functions (used in alarm groups)
2. Program alarm groups (if required) for access control functions
3. Select the door to program (in Access options)
4. Select Alarm control:
 - Enter the required alarm group
 - Select the required alarm control option
 - Select if the IN or OUT reader should deny access when the area is armed
 - Select the Authorised RAS on the system databus (if required)
5. Program the alarm groups for the Person Profiles that should have alarm control.

Anti-Passback

For anti-passback to function, readers are required to enter and exit. The reader address specifies if the reader is used as an IN (entry) or OUT (exit) reader (see “Numbering” in the *Alliance 8300 Online Help*).

To program anti-passback facilities:

1. Make sure both IN and OUT readers are available and are polled.
2. Select the door to program (in Access options)
3. Program Access options:
 - Select the required passback option (disabled, soft, or hard).
 - Enter the region number for the IN and OUT reader.
 - Select if the IN or OUT reader should not allow users from region 0.

Configuring DVRs and cameras

Refer to the *Alliance 8300 CCTV Interface Guide* and the *Alliance 8300 Online Help* for details.

Access rights, persons, and badges

A user (person with a badge) may gain access to areas, doors, or floors protected by the security system.

Alliance 8300 uses a number of concepts to control access rights, persons, and badges. This chapter describes these concepts.

Access rights

The process of controlling access begins with the three *access groups* — Alarm Groups, Door Groups, and Floor Groups — which define the relationship of alarms, devices (such as readers), and timezones to a control panel.

A Person Profile may be assigned no more than one Alarm Group, Door Group, and Floor Group per control panel.

For example, a Department Manager would require a particular set of access rights for Managers, and these could be assigned to him in his Person Profile record.

Alarm groups

Alarm groups provide the means to control the system intrusion alarm functions (also called alarm control). Alarm groups have areas and timezones, menu options, and panel options.

Alarm groups are assigned to Person Profiles, and therefore to each intrusion panel related to that alarm group for every person having the profile assigned.

Door groups

Door groups specify when access to a specific door or arming station will be granted. Door groups are assigned to users via the Person Profile.

Each door group may have a different time period (timezone) when access to the door or arming station will be granted.

Floor groups

Floor groups specify when access to a specific floor will be granted. Floor groups are assigned to users via the Person Profile.

Each floor group may have a different time period (timezone) when access to the door will be granted.

Person profile

A set of access rights for a particular category of person is determined by a type of record called a Person Profile.

Note: A Person Profile might be used by many people, and may be linked by badge group to many control panels. As a result, any change in a person profile can result in lengthy download times.

Person

The Person form is used to enter a person record into Alliance 8300 and assign access rights via a selected Person Profile.

Badges

Badge records are defined in Alliance 8300 from the Personnel > Badge menu entry.

A badge has a unique identity number. This is either a badge number and site code for known formats, or a 48-bit number (called Raw Card Data). In Alliance 8300, the term 'badge' also applies to a PIN (personal identification number) that is entered on a RAS keypad.

When a badge is assigned to a person, and it belongs to a badge group that is indicated for download to a control panel, the badge will be downloaded (sent) as a user to the control panel (and any associated four-door/four-lift DGP controllers), as long as the badge is 'active'. As a result of this association between badges and control panels, certain conditions control how users can be added to any system. These are:

- Each person-badge combination is represented by a 'user number' at the control panel.
- User numbers greater than 50 require a memory expansion module.
- User numbers above 11,466 require an IUM (Intelligent User Module) memory expansion module.
- In a system with 1 MB expanded memory, users numbers from 1,001 through 11,466 may have a badge only without a PIN.
- When using Soft IUM in combination with the 1 MB memory expansion, user numbers above 2,000 require an IUM (Intelligent User Module) memory expansion module (see also "Control panel memory" on page 68).
- In a system with 1 MB, 4 MB, or 8 MB expanded memory, only the first 200 user numbers can have their names programmed to their user number in the control panel (although in Alliance 8300 all users can have names).

Every new control panel that you create will have default badge groups listed according to the default types* selection that was made when the Alliance 8300 database was created.

* Each default type corresponds to a set of default hardware settings to provide for regional differences between control panels.

Badge groups

Badge Groups are defined in Alliance 8300 from the Personnel > Badge group menu entry.

See "Badge groups [A]" on page 2 for introductory information.

Badge groups tell the Alliance 8300 system which badges need to be downloaded to which control panels. Badge groups are linked to control panels via the Badge Groups tab of the Controller Setup form.

Alliance 8300 provides default badge groups to accommodate the following badge formats:

- ATS Wiegand 32 bit
- ATS Wiegand 30 bit
- Aritech Mag Stripe
- Hughs 34 bit
- PIN
- Raw data
- Tecom ASP
- Wiegand 26 bit
- Wiegand 37 bit
- HID C1000
- Master Installer Types (depending on the languages selected when the database was created)
- Master User Types (depending on the languages selected when the database was created)

Note: See “Master badge groups” below for information on MASTER Installers and MASTER Users.

Every new control panel that you create will have the default badge groups listed on the Badge Groups tab of the Controller Setup form.

Master badge groups

All new Alliance 8300 control panel records are created* with at least one ‘Master’ badge group:

- Master Installer type (assigned Badge No. 50) enables a new control panel to be programmed initially.
- Master User type (assigned Badge No. 1) enables a new control panel to be used for access initially. The Master User type does not apply to Australian database defaults.

* The “Master” badge group(s) may be removed from the new control panel record prior to saving the record. This is important for control panels with existing badge databases. See “Controller setup [A]” on page 2.

Note: Failure to remove Badge Groups named MASTER Installer Type or MASTER User Type prior to saving a new control panel record for an existing control panel (with existing users) may result in overwriting users 1 and 50 with the MASTER Installer or MASTER User types (as applicable).

It is further recommended that the MASTER badge groups are removed from the panel’s assigned badge groups as soon as they are not needed, for the following reasons:

- The master PINs may be used on the control panel, possibly resulting in unauthorised use.

- The existence of the master badges using badge numbers 1 or 50 (as applicable) can cause conflicts where an operator uses one of these badge numbers for a badge or PIN. If attempts were made to add the badge group to the panel, such a conflict could prevent all badges of the group from being downloaded to a control panel until it is resolved.

If you wish to have your own special Installer or User PINs, then you must create PIN-only records using the Badge Setup form. Assign the appropriate badge numbers (1 or 50) to use the same locations in the control panel memory as previously used by the default badge groups.

Each type of Master badge group has associated read-only records for Person, Person Profile, and Badge. For example, the Badge Group “MASTER Installer Type (Australia)” is the owner of the badge named “MASTER Installer PIN (Australia)”.

Assigning badge groups

Control panels are defined in Alliance 8300 from the Device > Advisor Master > Setup menu entry.

When a control panel is first defined, use the Badge Groups tab to define which badge groups are eligible* for downloading (sending) to the control panel.

* For a badge to be downloaded to a control panel, the following rules apply:

- The Badge Group must be assigned to the control panel.
- The Badge Group must be assigned to the badge.
- The badge is assigned to a person.

Notes

- Remove all unneeded badge groups before saving the new control panel record in Alliance 8300. See “Master badge groups” on page 66 for details.
- Before saving a new record for a control panel with existing users, remove the MASTER badge groups to avoid overwriting users 1 and 50.

Use the Badge Groups tab on the Controller Setup form to add or remove Badge groups that the control panel will use.

To edit the list, click Assign Badge Groups to display the Assignment dialog.

Select the required badge group in the Available list and move it to the Assigned list to add the badge group to the control panel.

Alternatively, select a badge group in the Assigned list and move it to the Available list to remove the badge group from the control panel.

When adding a control panel with the default badge groups, the default Master Installer and Master User will be downloaded to the control panel as users, along with any additional badges that have been assigned to the panel’s default badge groups. To prevent this, remove the badge groups prior to saving the record.

Control panel memory

The use of memory expansion modules governs the number of users available to Advisor Master control panels and Advisor Master four-door or four-lift DGPs.

Table 3: Number of available users for different memory types

Panel memory	Quantity of users
Small (no expansion)	50
Expanded (1 MB)	11,466
IUM Tiny (software IUM)	50
IUM Mini (software IUM)	2,000
IUM Small (4 MB hardware IUM)	17,873
IUM Expanded (8 MB hardware IUM)	65,535

Note: Advisor Master four-door or four-lift DGPs must be fitted with the same memory expansion modules as the associated control panel.

In Alliance 8300 the closest counterpart to control panel users are badges. In fact, a badge represents a collection of users across multiple control panels.

A badge will create a user record for a control panel under the following conditions:

- The badge is assigned to a person
- The badge belongs to a badge group that has associated control panels (users will only be created in those control panels)
- The badge is active

In control panels without memory expansion (non-IUM), the badge number directly corresponds to the user number in the control panel (therefore, the user number refers to the physical badge number).

In control panels with expanded memory (IUM), the badge number may or may not correspond with the user number in the control panel (raw card data is used, not the badge number). For these control panels, Alliance 8300 applies the following rules:

- If a matching user number is available, the user number and badge number are the same.
- If a matching user number is not available, Alliance 8300 selects the first available user number in the control panel starting from 1 and working up to the maximum permitted by the control panel's user memory.

Note: Use the Badge to Users report to identify the assignment between badges and user numbers on all applicable control panels.

Learning badge data

The Learn Badge Data form is used to search the Alliance history database(s) for unknown badge data from one or all badge learn devices (badges that are known to the system do not need to be learned).

The overall process for learning badge data is as follows:

1. Use the Badge learn tab on the Parameters form to specify the device(s) to be used for learning badges.
2. On the Badge Setup form, click the Learn button to open the Learn Badge Data form.
3. On the Learn Badge Data form, click the Learn device arrow and select the required device, or use the default <ALL LEARN DEVICES> to search all learn devices available to the operator.
4. Click the Facility arrow and select a facility to limit the search. This field is active only when <ALL LEARN DEVICES> is selected.
5. Click the Time window arrow and select the required time and date settings (hardware date and time) for the search. Depending on the dates selected and the archive database settings on the Parameter form, you may need to select Include Archive database in search.
6. After specifying the search criteria, or accepting the default settings, click Find to perform the search. The label on the button changes to Refresh. If any search criteria is changed, click Refresh to update the badge data list.
7. Select the required unknown badge data, and then click OK to learn the raw badge data into Alliance 8300. When the badge learn process is complete, the badge data is displayed in the 'Raw badge data' field on the Badge Setup form.

Detailed instructions are contained in the *Alliance 8300 Online Help*.

Controlling operations

This chapter deals with the tasks associated with the Alliance 8300 Operations menu.

Refer to the *Alliance 8300 Online Help* for more details about these options.

Some options have corresponding toolbar buttons — these are indicated below the heading (as applicable).

Managing control panels

Controller utility



The Controller Utility allows you to monitor control panel state and issue commands to one or more selected control panels using either Controller Utility toolbar or right click shortcut. In the following list, commands are available from both the toolbar and right click shortcut except where noted.

The Controller Utility form provides commands for devices. Not all commands may be available for particular devices. Possible commands are:

- **Edit:** Edit the properties of the selected control panel using the Controller Setup form.
- **New:** Define a new control panel using the Controller Setup form.
- **Change state:** Set the selected offline control panel online, or set the selected online control panel offline.
- **Dial/Hangup:** Enabled only when the selected intrusion control panels are dial-up type, and have the same connection status (for example, currently connected). A dial or hangup command applies to all selected control panels.
- **Download >Badges Database:** Send the badges database to the selected Advisor Master control panels.
- **Download > Installer Database:** Send the installer database to the selected Advisor Master control panels.
- **Download >Full Database:** Send both the badges and installer databases to the selected Advisor Master control panels.
- **Upload > Installer Database:** Receive the installer database from the selected Advisor Master control panels.
- **Upload > Door/Floor Groups, Holiday Database (right click shortcut):** Receive the door groups, floor groups, and holiday database from the selected Advisor Master control panels.

- Upload > Full Database: Receive the installer database and the door/floor groups, and holiday database from the selected Advisor Master control panels.

Note: Uploading of the badges database is not supported in the current release of Alliance 8300. However, if a PIN has been changed on a keypad for an existing badge in the database, the new PIN is uploaded, the related badge details updated and propagated to all panels in the network.

- Accept Events (right click shortcut): The default setting is enabled, where the Accept Events menu item is marked with a tick and events sent by the Advisor Master control panel are received by Alliance 8300. The control panel may still be connected but events are not processed by Alliance 8300. See “Accepting events” below for details.
- Queue Outgoing (right click shortcut): The default setting is disabled, and commands are transmitted from Alliance 8300 to the Advisor Master control panel. When selected, a tick appears next to the Queue Outgoing menu item. The control panel may still be connected but outgoing commands from Alliance 8300 to the control panel are suspended and queued until the Queue Outgoing is set to disabled. See “Queuing outgoing events” below for details.
- Date and Time (right click shortcut): Opens the Date and Time Control form for the selected Advisor Master control panels. Select multiple control panels to set the local date & time for all selected control panels simultaneously. This setting will be displayed on local RAS LCD displays and reported to management software.
- Engineering Reset (right click shortcut): Opens the Engineering Reset Control form for a selected Advisor Master control panel.
- Remove Controller Panels (right click shortcut): Hides the selected control panel(s) from the list. To restore, close and re-open the Controller Utility form.

Accepting events: Right click the Controller Utility form to clear the Accept Events setting. Clearing this setting causes Alliance 8300 to suppress receiving events from the Advisor Master control panel. Some reasons for suppressing events are:

- You might want to upload (receive) the full database from the control panel before accepting events. Doing so enables Alliance 8300 to learn details of the alarms to be reported.
- An installer may need to connect to a control panel for maintenance without accepting events.

Queuing outgoing events: Right click the Controller Utility form to select the Queue Outgoing setting. This setting causes Alliance 8300 to suppress sending data to the Advisor Master control panel. Some reasons for queuing outgoing data are:

- Allow operators to make configuration changes without the changes being sent prematurely by Alliance 8300.

- Allow installers to make all necessary configuration changes, and apply those changes during times of low risk.

Monitoring badges

Badge Monitor



The Badge Monitor command opens the Badge Monitor form that allows the operator to monitor badge activity (according to the operator's facility assignment, see "Operator interface" on page 20).

In the following list, commands are available from both the toolbar and right click shortcut except where noted.

The Badge Monitor commands are as follows:

- Resume: Starts the scrolling of badge activity. This command is active only if you pressed the Pause button. All badge activity that occurred while the Pause command was on will be displayed once you select resume.
- Pause: Suspends the scrolling of badge activity on the Badge Monitor.
- Clear: Clears all badge activity from the Badge Monitor.
- Badge... (right click shortcut): Opens the Badge form.
- View Live Video (right click shortcut): For a selected badge transaction with a camera icon displayed, use this shortcut to automatically access live video from camera(s) associated with the door/RAS's badge transaction, as defined by its event trigger.

Note: The DVR must be online and in record mode.

- View Recorded Video (right click shortcut): For a selected badge transaction with a camera icon displayed, use this shortcut to automatically playback recorded video from camera(s) associated with the reader's badge transaction, as defined by its event trigger.

Note: The DVR must be online and not in error condition or serving another request for playback of recorded video.

- Quick Launch (right click shortcut): For a selected badge transaction with a camera icon displayed, use this shortcut to automatically access live video and playback recorded video from camera(s) associated with the door/RAS's badge transaction, as defined by its event trigger.
- Swipe & Show: Shows additional details on badge transactions for assigned Swipe & Show readers. Details include person last & first name, profile, region, picture (when available) and badge history. If a valid event trigger is set, live camera images will show next to the Swipe and Show form.
- Assign Swipe & Show Readers: Identifies for which readers Swipe & Show data should automatically be shown.

Notes

- The DVR must be online and not in error condition or serving another request for playback of recorded video.
- A badge activity must have a DVR association in order to enable video options on the right click menu. Camera and door/arming station association (linking) is accomplished using the menu Administration > Event Trigger.

Monitoring alarms

Alarm Monitor



The Alarm Monitor displays alarm (input) activity. An alarm is displayed on the Alarm Monitor if the Monitor field was selected in the Alarm form.

Fire alarms will be shown in a separate section for Fire alarms only. All other events from all devices, including fire alarm systems, will show in the general alarm section. To view Fire Alarms, click the Fire Alarms button in the Alarm Monitor (only enabled if Fire Alarms are present).

All acknowledgments are recorded in both Operator and the Alarm History. In addition, all responses are recorded when the alarm is acknowledged.

There are three sections to this form:

- The top section or pane lists the alarms.
- The second pane lists any alarm instructions assigned to the current (highlighted) alarm.
- The third pane allows you to respond to an alarm by either selecting a predefined response or entering your own.

In the following list, commands are available from both the toolbar and right click shortcut except where noted.

The Alarm Monitor commands are as follows:

- Remove All (toolbar): Remove all alarms on the Alarm Monitor regardless of whether the alarms are acknowledged or unacknowledged as long as it was not defined on the Alarm form as requiring an acknowledgment. An operator must have an ALL permission for the Alarm Monitor in order to have access to this icon.
- Remove Individual (toolbar): Remove one or more alarms without waiting for them to reset. The alarms can be unacknowledged and cleared as long as it was not defined on the Alarm form as requiring an acknowledgment.
- Show Inactive Alarms (right click shortcut): For tracking purposes, you may select Show Inactive Alarms to display previously acknowledged alarm states that have not yet been removed from the display.
- Alarm: Right click shortcut to the Alarm form.

- Alarm Graphics Viewer: Right click shortcut to the Alarm Graphics Viewer form
- Alarm Graphics Editor: Right click shortcut to the Alarm Graphics Editor form.
- View Live Video (right click shortcut): For a selected alarm transaction with a camera icon displayed, use this shortcut to automatically access live video from camera(s) associated with the alarm's transaction, as defined by its event trigger.

Note: The DVR must be online and in record mode.

- View Recorded Video (right click shortcut): For a selected alarm transaction with a camera icon displayed, use this shortcut to automatically playback recorded video from cameras associated with the alarm's transaction, as defined by its event trigger.

Note: The DVR must be online and not in error condition. For DVR range it may not be serving another request for playback of the recorded video.

- Quick Launch (right click shortcut): For a selected alarm transaction with a camera icon displayed, use this shortcut to automatically access live video and playback recorded video from cameras associated with the alarm's transaction, as defined by its event trigger.

Notes

- The DVR must be online and not in error condition. For DVR range it may not be serving another request for playback of the recorded video.
- An alarm activity must have a DVR association in order to enable video options on the right click menu.
- Fire Alarms (toolbar): Shows Fire Alarms only (other events from the Fire Alarm System will show in the general alarm monitor view). Only enabled when Fire Alarms are present.

Combined monitoring

Live History Log



The Live History Log allows the operator to monitor badge activity (according to the operator's facility assignment, see "Operator interface" on page 20), alarms and events.

Use the toolbar to select filters (the types of events to monitor) and to control the display of events in the window. In the figure below, only the Valid badge button (item 7) is shown as selected.

Figure 13: Live History Log toolbar



1. Resume: Starts the scrolling of events. This command is active only if you have selected Pause. All events that occurred during pause will be displayed once you select resume.
2. Pause: Suspends the scrolling of events on the Live History Log.
3. Clear: Clears all events from the Live History Log.
4. Active: Show alarms.
5. Inactive: Show alarm resets.
6. Trouble: Show fault events.
7. Valid: Show valid badge transactions.
8. Invalid: Show invalid badge transactions.
9. Lost: Show lost badge transactions.
10. Overdue: Show overdue (expired) badge transactions.
11. Unknown: Show unknown badge transactions.
12. Close: Show door close commands.
13. Open: Show door open commands.
14. Lock: Show door lock commands.
15. Unlock: Show door unlock commands.
16. Trace: Show traced user events.
17. Select all: Show all events.
18. Deselect all: Show no events.
19. Refresh: Update window.

Right click functions depend on the type of the selected event. For alarms, please refer to the “Alarm Monitor” on page 73. For badges, see “Badge Monitor” on page 72.

Creating and using alarm maps

Alarm Graphics Editor

The Alarm Graphics Editor allows an authorised technician to create a map (graphical view) of alarm states for the alarms you select, and to create links to other maps. For example, the operator might start off with a facilities map with an alarm point on a building. If the alarm point has been defined as a jump to the building’s map, clicking the icon will display the building map, and so on. Jump points to other maps do not need to be linked to an alarm.

A map has a background image, which can be a bitmap, a vector drawing, or a combination of both bitmaps and vector drawings, saved in Windows MetaFile (.WMF), Enhanced MetaFile (.EMF), Joint Photographic Experts Group (.JPG), or Bitmap (.BMP) format.

Applications such as Microsoft Visio, Microsoft PowerPoint, CorelDraw, Adobe Illustrator, and many other drawing applications can save images in any of these formats. The same background image file may be used to create a number of different map files by using different views and different magnifications of the background, with different alarm, camera, and jump points superimposed.

Alarm Graphics Viewer



The Alarm Graphics Viewer command opens the Alarm Graphics Viewer that allows the operator to view maps created in Alarm Graphics Editor. These maps indicate the location and type of incoming alarms.

Use the Alarm Graphics Viewer to select and display an alarm graphics map. Maps can contain icons that represent the physical locations of one or more devices such as doors or cameras. The icons can change appearance to indicate conditions of trouble, alarm, or reset.

An icon may be linked with another map (for example, to display a room within a building). Click a linked icon to view the other map.

Managing clients

See “Managing network client computers” on page 82 for details about this topic.

Managing zones

Zone Control

Select Zone Control to display a list of zones by All Controllers, or select to filter the list By Controller.

Select from the predefined Purposes or type a Purpose text to describe the reason for the command. These comments are written to the operator history file and appear in the purpose field of the Operator History report.

Click the zone you want to control, and then select a function (Inhibit, Uninhibit, Reset, or Reset ACK). The command will be sent to the control panel.

Zone Status

Provides the status of the selected zones by All Controllers, or By Controller. The lists may be filtered by your assigned operator facilities (see “Operator interface” on page 20 for details).

Click the Get Status button to get an updated status on the selected zone. This may take a few minutes if a dial-up control panel is not currently connected.

Managing doors

Door/Output Control



The Door/Output Control command allows you to manually open or close doors and turn on or off outputs.

You can list readers (these are also referred to as arming stations or doors) or outputs for all control panels (or per control panel), as listed in the Controller Utility form.

The labels of the Set state to buttons change depending on whether Reader or Other is selected.

Select from the predefined Purposes, or type a Purpose text to describe the reason for the command. These comments are written to the operator history file and appear in the Purpose field of the Operator History report.

“Reader” commands: When the selected DO type is Reader, (arming stations or doors) the associated commands are:

- Duration Unlock: Opens the Timed Open window. Enter the time in seconds for the duration unlock time, and then click OK.
- Indefinite Unlock: Unlocks the highlighted door, which will remain unlocked until you manually lock it by clicking Lock.
- Open: Immediately unlocks the highlighted door.
- Lock: Immediately locks the highlighted door.
- Enable: When the Enable button is clicked, the selected devices will be enabled and will respond to all valid commands such as Open or Lock.
- Disable: When the Disable button is clicked, the selected devices will be disabled and will not respond to commands such as Open or Lock.

“Other” commands: When the selected DO type is Other (outputs) the associated commands are:

- On Indefinite: Activates the highlighted output, which will remain active until you manually turn it off by clicking Off.
- Off: Deactivates the selected device.

Door/Output Status

The Door/Output Status screen displays the current state of the selected door or output, as received from the control panel.

Click Get Status to send a request for updated information from the control panel.

Managing high security regions

Use the High Security Regions form to control doors assigned to the High Security Regions (HSR).

Select doors to control with assigned required High Security Users (HSU) on list by All Controllers, or select to filter the Doors with assigned required HSU list By Controller. The doors available for your control display in the door list, as permitted by Operator Facilities assigned to you.

Click Check Status to get the states of the High Security Regions that doors are assigned to.

Type up to ~20 words in the Purpose text box to describe the reason for the command. These comments are written to the operator history file and appear in the purpose field of the Operator History report.

Select High Security Regions you want to control, and then click proper command (Stop Alarm or Reset Number of users).

Managing lifts

Lift Control

Use the Lift Control form to display a list of lifts for all of your assigned control panels, or for a selected control panel.

Click the Select Lift arrow and select a lift from the list. The associated lift number, floor number and control panel description are displayed in the list.

Click the floor that you want to control, and then select a function (Disarmed or Armed). The command will be sent to the control panel.

Select from the predefined Purposes or type a Purpose text to describe the reason for the command. These comments are written to your operator history file and appear in the purpose field of the Operator History report.

Lift Status

Use the Lift Status form to display a list of lifts for all of your assigned control panels, or for a selected control panel.

Click the Select Lift arrow and select a lift from the list. The state of the Lift and its floors are displayed in the list, as received from the control panel.

Click Get Status to send a request for updated information from the control panel.

Managing areas

Area Control

Select Area Control to display areas by All Controllers, or By Controller. The lists may be filtered by your assigned operator facilities (see "Operator interface" on page 20 for details).

Select from the predefined Purposes or type a Purpose text to describe the reason for the command. These comments are written to the operator history file and appear in the purpose field of the Operator History report.

Click the Area you want to control, and then select a function (Arm, Forced Arm, or Disarm). The command will be sent to the control panel.

Area Status

Select Area Status to display areas All Controllers, or By Controller. The lists may be filtered by your assigned operator facilities (see “Operator interface” on page 20 for details).

The Area Status screen shows the current state of the selected Areas, as received from the control panel. Click Get Status to send a request for updated information from the control panel.

Managing arming stations

Arming Station Control

Select to display an Arming Stations list by All Controllers, or By Controller. The lists may be filtered by your assigned operator facilities (see “Operator interface” on page 20 for details).

Select from the predefined Purposes or type a Purpose text to describe the reason for the command. These comments are written to the operator history file and appear in the purpose field of the Operator History report.

Click the Arming Station you want to control, and then select a function (Inhibit, Uninhibit, or Door Open). The command will be sent to the control panel.

Arming Station Status

Select to display an Arming Stations list by All Controllers, or By Controller. The lists may be filtered by your assigned operator facilities (see “Operator interface” on page 20 for details).

The Arming Station Status screen shows the current state of the selected Arming Stations (RASs), as received from the control panel. Click Get Status to send a request for updated information from the control panel.

Managing DGPs

DGP / Controller Control

Select to display a DGP list by all controllers, or by controller. The lists may be filtered by your assigned operator facilities (see “Operator interface” on page 20 for details).

Select from the predefined Purposes or type a Purpose text to describe the reason for the command. These comments are written to the operator history file and appear in the purpose field of the Operator History report.

Click the DGP you want to control, and then select a function (Inhibit, Uninhibit, or Battery Test). The command will be sent to the control panel.

DGP / Controller Status

Select to display a DGP list by all controllers, or by controller. The lists may be filtered by your assigned operator facilities (see “Operator interface” on page 20 for details).

The DGP Status screen shows the current state of the selected DGPs, as received from the control panel. Click Get Status to send a request for updated information from the control panel.

Managing time locks (TML)

TML Control

Before commencing the control commands described below, all the correct Bank DGP needs to be selected in the left hand window of this control menu.

- Inhibited TMLs: Used to inhibit or uninhibit the TMLs.
- Allow Vault Sensor: In case one or more TMLs are inhibited allows that the vault sensor is still operational.
- Solenoid override: Used to override the solenoid detection switch when not used.

In the Purpose field, enter a comment explaining the reason for changing the TML states. These comments are written to the operator history file and appear on the Operator History Report, Purpose Field.

Managing Fire Alarm Systems

FAS Control and Status

Fire Alarm Systems functionality is described in the *Alliance 8300 FAS Reference Guide*.

Managing digital video

Digital Video Viewer



The Digital Video Viewer menu item under the Operations Menu opens a video command and control application that allows you to monitor digital video multiplexers/recorders and their associated cameras, control live video, as well as search and play back recorded video events.

Changing your password

The Change Password menu opens the Change Password form which allows you to change your password.

Selecting facilities

The Select Facilities command opens the Set Active Facilities form which allows you to change the facilities currently in use.

Performing engineer walk test or user walk test

These menus allow the user or engineer to start the walk test and to monitor its progress.

Select the areas and then start the test.

The list “Zones To Test” provides users with a list of untested zones. The zone assigned to the selected area will be included into this list, only if the Engineer Walk Test or User Walk Test in the Zone Database is enabled for this zone.

It is assumed that Alliance database is synchronized with the panel’s database so that Alliance can determine the same list of zones to be tested.

As “zone tested” events are received from the panel, the particular zones will be moved from the list of untested zones to the list of tested zones.

The Walk Test State can indicate one of the following.

Table 4: Possible walk test states

State	Description
Unknown	Status unknown
Idle	Ready to start the test
In use	Busy, other test execution is already in progress
Started	Test request sent
In progress	Test request accepted, test in progress
Canceled	Cancel test request sent
Succeeded	Test finished, success
Failed	Test finished, failed or canceled

See the appropriate control panel programming manual for more details.

Camera footage on alarm

Select this option to automatically display camera footage on alarm, if a corresponding trigger is defined. The video window will be displayed until an operator will close it manually.

Managing network client computers

In order for your networked clients to connect to the server computer, the server computer must know who they are. You may refer to the Client Monitor form to obtain client type, Imaging status, and connection status. You may use the Client form to add, modify, and remove computers from the network.

Client Monitor form



Open the Alliance 8300 Client Monitor form from the Operations > Client Monitor menu or click the toolbar button displayed at left.

The Client Monitor command opens the Client Monitor form, which allows you to obtain client information such as client type (Alliance 8300 or CCTV), Imaging status, and connection status.

Figure 14: Client Monitor form

Client	Client Type	Imaging status	Connection status	Description	Primary Com Port	Secondary C
INFRA_39M783J (DBServer)	A8300 Client ...	Enabled	Connected	PCName	NULL	NULL
PC_NUM1	A8300 Client ...	Disabled	Not connected	PC_NUM1	NULL	NULL
PC_NUM2	A8300 Client ...	Disabled	Not connected	PC_NUM2	NULL	NULL

Connection Information

Licenses used: 1

Client licenses: 5

Imaging Information

Licenses used: 1

Imaging licenses: 1

The top of the Client Monitor form displays all currently defined network clients, their Imaging status, and their connection status.

The Imaging status is either Enabled or Disabled. If enabled, this client counts as taking an Imaging license. You cannot enable Imaging on more network clients than you have Imaging licenses. The Imaging license allows you to capture images and signatures, create badge designs, and print badges. Without a license, you cannot create badge designs and print badges.

The connection status is either Connected or Disconnected. If the network client is disconnected, it is not added to the number of active licenses; the number of active licenses is only increased if the client is connected. To connect the client, log in on that computer. An application running on the Server computer counts the licenses used.

The bottom of the Client Monitor form displays the number of licenses currently in use along with the total number of licenses allowed.

In the following list, commands are available from both the toolbar and right-click shortcut except where noted.

The Client Monitor commands are as follows:

- **Disconnect Client:** Disconnects the selected client.
- **Launch Client:** Select this icon to enable a CCTV interface (currently not enabled).
- **Client form:** Right click shortcut to the Client form to, for example, enable or disable Imaging for the particular Alliance 8300 client.

Note: When using the Launch Client command, you must restart the Alliance 8300 computer to enable the CCTV interface.

Client form

Use the Client form to define a client computer.

Open the Alliance 8300 Client form from the Administration > Client menu.

Adding clients

You can add clients that are already set up on the network. When you click the Browse button, you receive a view of all computers that Alliance 8300 can find on your network. Select the ones you wish to use.

You can add as many clients as you want. However, only the licensed maximum can connect to the server at the same time. For specific features of the Client form, refer to the *Alliance 8300 Online Help*.

Modifying/removing clients

To remove a client from the network, it must be disconnected. This can be done by having that client exit, or by selecting the client on the Client Monitor form and clicking Disconnect on the toolbar, or selecting Disconnect from the shortcut menu of the Client Monitor form. You **MUST** have a permission action of All, which is set on the Permission form, in order to disconnect clients.

You can enable or disable Imaging on a client without disconnecting it. You may have more Imaging stations set up than you have licenses. However, if not all the clients require the license at the same time, you can enable and disable the license for the appropriate clients.

Reports and templates

This chapter discusses reports and templates for the reports. Alliance 8300 provides extensive reporting capabilities based on your system configuration. All reports are selections of the Reports menu.

Note: Reports are filtered so that supplied information pertains only to the selected facilities of the current user.

Reports

For complete details of fields and capabilities of each Report, refer to the *Alliance 8300 Online Help*.

Note: Be careful when selecting font styles and sizes. Some styles may not appear as desired when printed and some sizes may be too large for the page. Use the Print Preview command to check how the font style and size will print on a page.

Fourteen standard reports are provided. Four are history reports. In addition, Alliance 8300 has the ability to access reports you have created using a third party report generator. The following is a brief description of each report.

Standard reports

Person

Provides personal information, such as address, department and person profiles, on all or a subset of persons in the system. Also provides an information for reports regarding badges assigned and regions.

Badge

Provides information on badges on all or a subset of badges in the system. Includes a report to relate Alliance badges to Advisor Master users.

Administration

Generates reports about the administrative options of the system. Report types include alarm instruction, archive, client, facility, host parameter, operators, permission, and response.

Advisor Master

Generates reports about the Advisor Master control panel devices in the system.

Floor Access

Lists the people who have access to floors.

Door Access

Provides a list of persons who have access to the specified door(s) or RAS(s); that is, who has access where.

Area Access

The area access report is a list of persons' levels of control over areas (i.e. the ability to secure, disarm and/or reset), listed by areas and by last name.

A person's level of control is determined by the options selected in the alarm groups assigned to the person profile.

Advisor Master Groups

Generates reports about the Door Groups or Floor Groups in the system, for a selected control panel or for all control panels.

Roll Call

Provides a list of persons showing the last access granted through a door ; that is, who last went where based on individual badge activity.

FAS Devices

Reporting on Fire Alarm Systems is described in the *Alliance 8300 FAS Reference Guide*.

History reports

By default both history and archive databases are used in history reports. The history database contains only records for the past day, week, or month as specified in "Archive Database" on page 46 (the default archive period is daily). All others are contained in the Archive database until cleared.

If data from the history or the archive only is required, select the required setting in the Database section. The dates selected in the date range need to match the database selected to retrieve valid output.

Alarm History

Generates reports on events reported to Alliance 8300. Most commonly these are alarm events

Select the required database and date range settings as described in "History reports" above.

Badge History

Generates reports on badge transactions.

Select the required database and date range settings as described in "History reports" above.

Time and Attendance History

Generates reports on time and attendance transactions.

Select the required database and date range settings as described in "History reports" above.

The use of time and attendance transactions in producing meaningful reports depends on the following:

- An Advisor Master four-door DGP (for example, ATS1250) must be used for time and attendance transactions.
- Doors reporting time and attendance transactions must have Time Attendance Reader selected on the Alliance Doors Setup form > Reader Options tab.
- Readers or keypads designated for time and attendance transactions must be used for entry to and exit from the workplace, and no other purpose (for example, accessing other parts of the workplace during work time).
- Badges or PINs used for time and attendance transactions must be used by only one person (however, a person may have multiple badges or PINs).
- A time interval beginning with an IN transaction is deemed to be “on site”.
- A time interval beginning with an OUT transaction is deemed to be “off site”.
- The difference between an IN transaction and the next following OUT transaction is deemed to be “work time”.
- Time and attendance transactions are records of badge or PIN use at specified readers. Such transactions are not necessarily records of work or absence from work by a person.

Operator History

Generates reports on operator actions.

Select the required database and date range settings as described in “History reports” on page 85.

External Reports

The External Reports command opens the Launch External Reports window, allowing you to access an executable application or report that was not created within Alliance 8300.

For example, you may wish to access a report created by a third party report generator such as Crystal Reports or Microsoft Access 2000 or 2002. Refer to “Using Microsoft Access 2002” on page 88 for instructions to create a project, connect with Alliance 8300, and create reports.

Templates

Alliance 8300 provides templates that allow you to enter report parameters. These can be saved and then recalled to run a report.

When you select a specific Report from the Alliance 8300 menu, a Template list box displays the name of the currently loaded template, if there is one. To select a template, click on the arrow at the right end of the field, which displays a list of the available templates. Select the desired template and it will be loaded.

Report templates are useful when a certain report will be run frequently. Once the desired report is selected, it can be saved as a template and revised by loading it from the template combo box.

If a date or time is specified, the date and time selections are saved as part of the template. You may need to change these areas each time you run the report. Verify that the template reflects the appropriate information and update as necessary.

Templates Button

The Templates button is for saving a template or making it a default.

Print Preview Report

The File > Print Preview Report command allows you to preview a report before printing it.

A printer must be set up in Windows and added to your system in order for this feature to work.

Print Report

The File > Print Report command allows you to send the current report to the currently defined printer.

Using Microsoft Access 2002

This section details the advanced procedures for creating database projects in Microsoft Access 2002 (MS Access) and connecting to Alliance 8300 databases.

The use of MS Access is not required for using Alliance 8300 — MS Access is only necessary to perform further maintenance on the databases or to create custom reports.

The first thing that must be done is to create the required SQL user named “exreport”. Microsoft Access 2002 reports created using other SQL logins may not achieve the desired results.

Creating the “exreport” user

The Alliance 8300 databases are initially installed with the system administrator user name “sa”.

The “sa” user name and password is used initially in MS Access 2002 only to create the required SQL user named “exreport”. The “exreport” user name is then used to set up the three Alliance 8300 database projects.

The “exreport” login has read-only permission to the three Alliance 8300 databases. This is the login that must be used to connect to the Alliance 8300 databases when using the Alliance 8300 Reports > External Reports command.

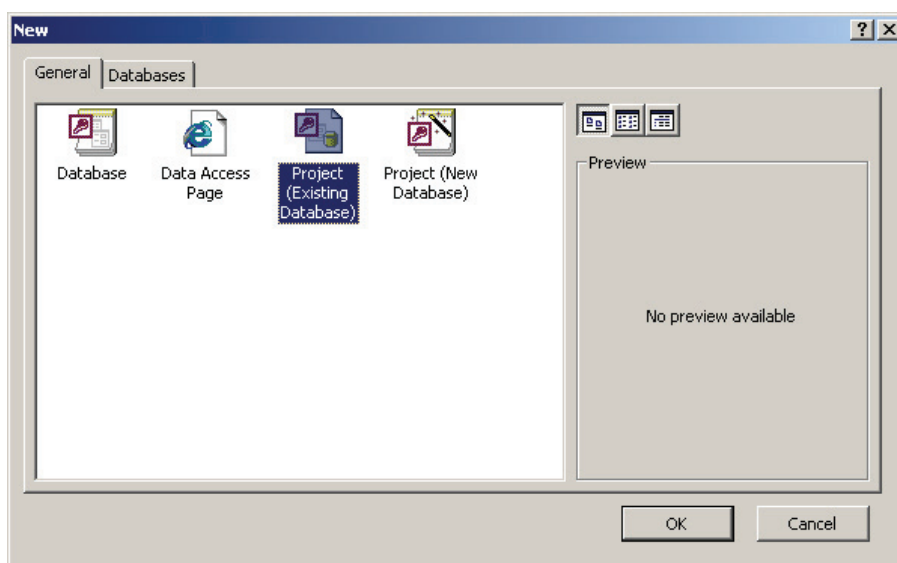
The password for the “exreport” login is setup using the Database Maintenance application (see “Changing the “exreport” password” on page 133).

Creating an MS Access Project

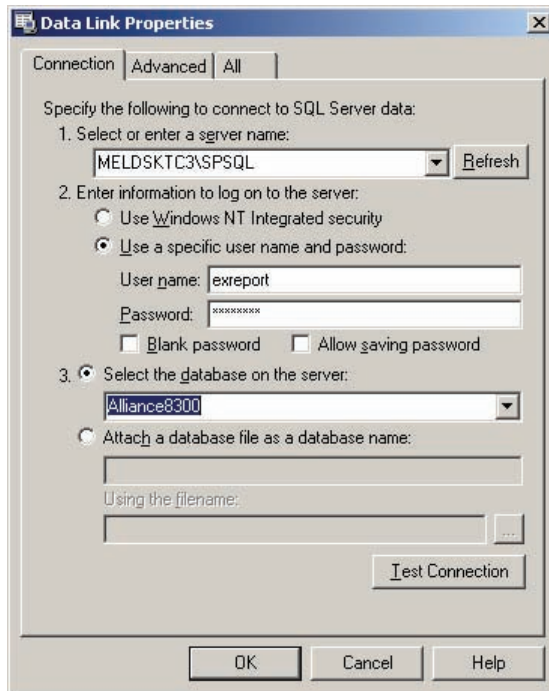
Begin by creating the Alliance8300 project and storing the project in the Alliance 8300 Database folder.

To create a new Alliance8300 project in MS Access:

1. In Access, select File > New > Project (Existing Database).



2. Click OK. A File New Database, Save In dialog box displays.
3. Name your project Alliance8300.adp and save in the Alliance 8300 Database folder (typically C:\Program Files\UTC Fire & Security\Alliance 8300\Database\).
4. Click Create. The Connection tab of a Data Link Properties dialog box displays, enabling you to link the newly-created MS Access project to an MS SQL database.



Connecting to the database

To connect the new project to Alliance 8300:

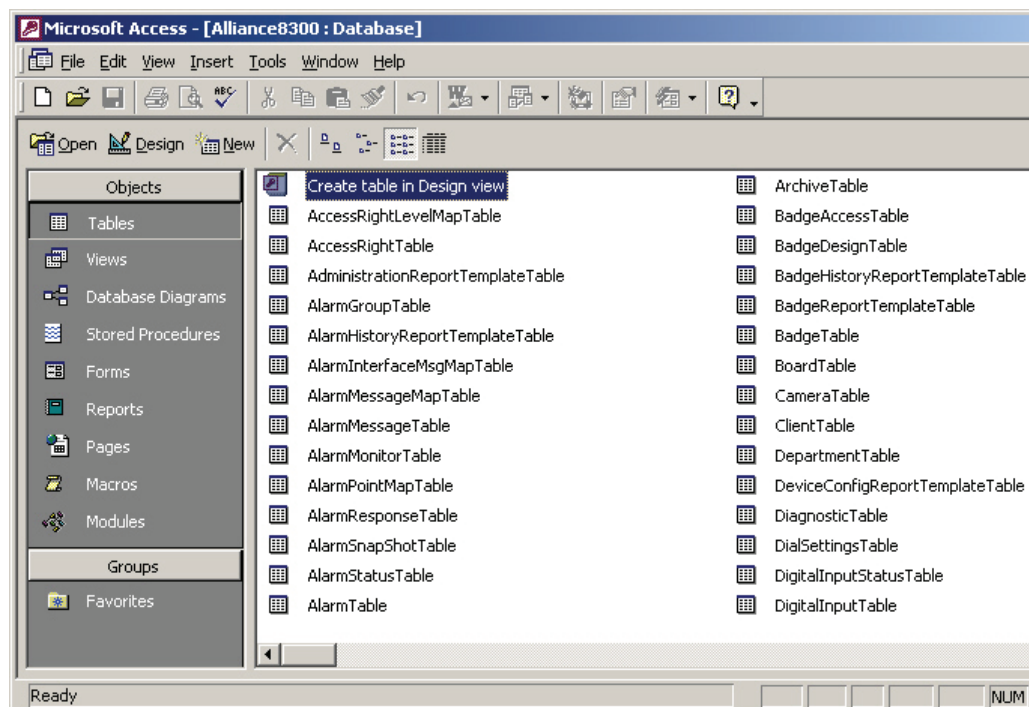
1. In the Select or Enter a Server Name field of the Data Link Properties, Connection tab, select your server name from the list.
2. Select Use a Specific User Name and Password, and type the user name “sa” and the password.
3. Do not select Allow Saving Password.
4. Choose Select the Database on the Server. Click the arrow and select Alliance8300.
5. Click Test Connection. A Microsoft Data Link dialog box displays, informing you the link was successful.



If the link was not successful, repeat these steps, verify your settings, and test the connection again.

6. Click OK.

Result: An Alliance8300.adp project is created and a list of the tables will display.



Setting up MS Access Reports for Alliance 8300

MS Access 2002 is required initially for creating the appropriate database user name and privileges (see "Creating the "exreport" user" on page 88).

Note: Use only MS Access 2002 to create the "exreport" user. It may be possible to use other versions of MS Access, such as Access 2000, for routine reporting tasks, however, some functionality may be lost or unavailable (depending on the version of MS Access and the Microsoft Service Release applied).

Creating an MS Access Project

Note: MS Access can be installed on the Alliance 8300 Server computer and/or any Alliance 8300 client computer.

An MS Access project must be created for each of the three Alliance 8300 databases:

- Alliance8300
- Alliance8300Archive
- Alliance8300History

Begin by creating the Alliance8300 project and storing the project in the Alliance 8300 Database folder.

Create a new Alliance8300 project as it is described in "Creating an MS Access Project" on page 88, but with a different user name ("sa") and password in step 4.

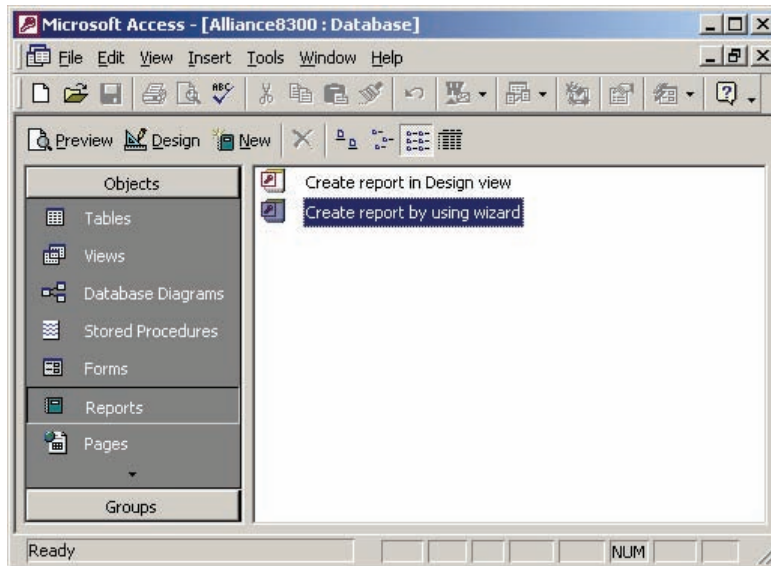
Note: Repeat the above steps to create all three projects, selecting at step 4 Alliance8300Archive, and again to select Alliance8300History.

Creating an MS Access Report

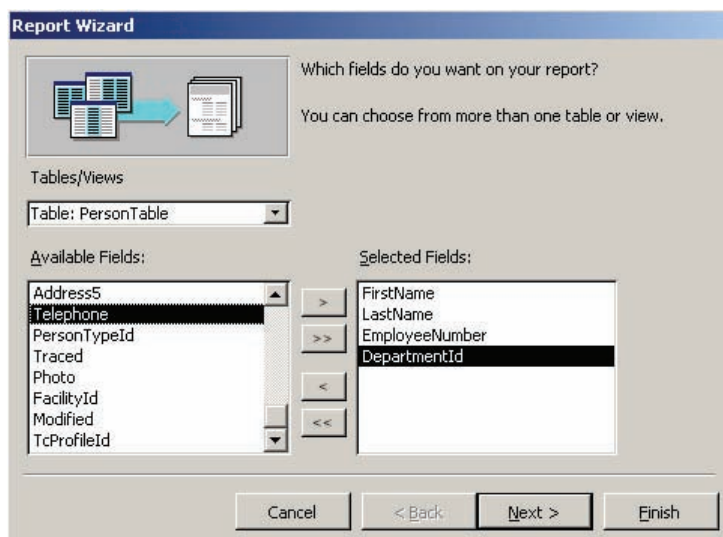
In this section, you will create an MS Access report using the Create report by using wizard utility, and then use drag-and-drop to automatically create a shortcut to the report for use by Alliance 8300.

To create and link a report to Alliance 8300:

1. In Access, click Reports in the Objects panel and then double-click Create report by using wizard.

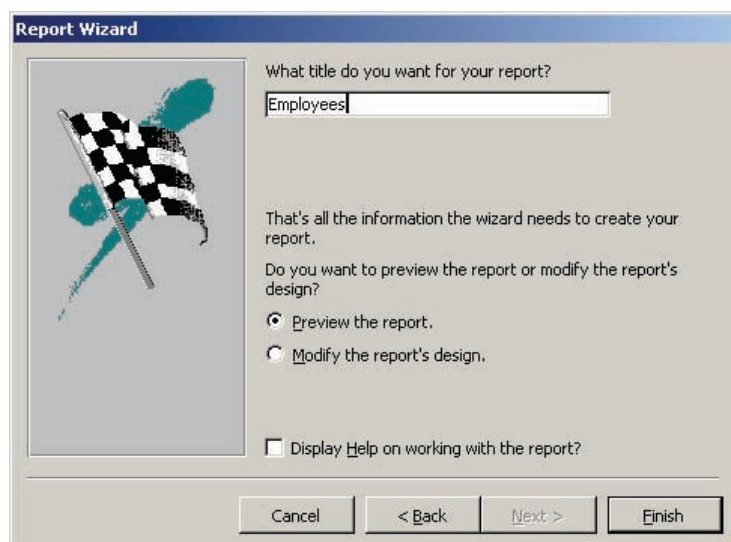


2. Follow the Report Wizard prompts to define a report. In the following steps, we'll create a sample personnel list.

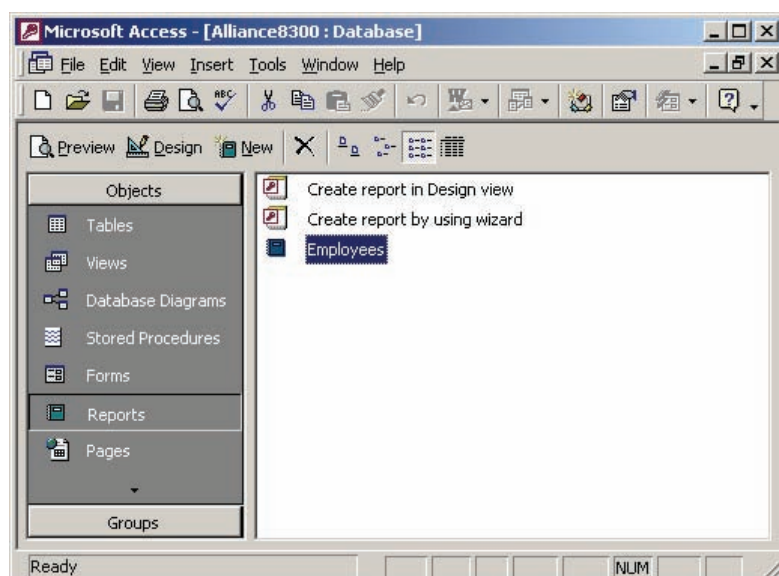


3. Click the Tables/Views arrow and select a table from which you want data.

4. Select fields from the Available Fields list and then click the right-facing arrow > to populate the Selected Fields list. Selected fields will be used in the report.
5. Subsequent steps in the Report Wizard allow you to group and sort the report data, layout the report format, select from pre-defined styles, and give it a title.



6. Click Finish.
7. Use the print preview and design views, if needed, to further customize the report. The report is listed in the MS Access Reports list.

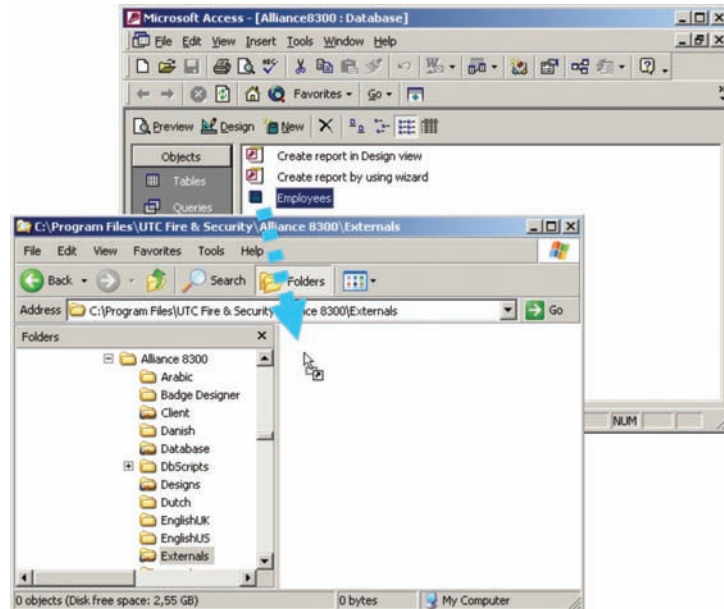


Do not close MS Access for now. You will use the Reports objects view in the next section (reduce the MS Access window size so that it does not occupy the entire Windows desktop).

Linking an MS Access Report to Alliance 8300

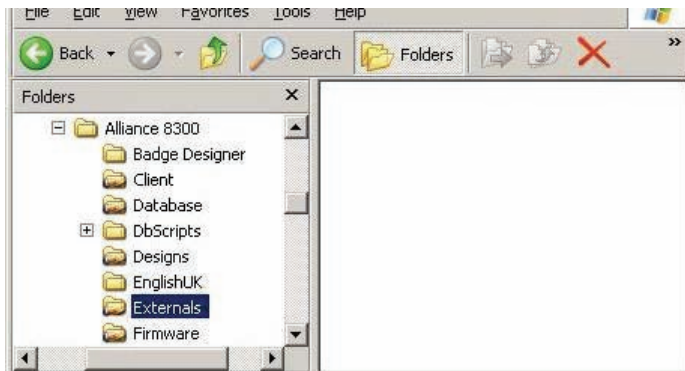
Alliance 8300 has been designed to allow you to quickly add MS Access reports to the Reports > External Reports command by means of Windows drag-and-drop functionality (see Figure 15 below).

Figure 15: Drag-and-drop method of creating a shortcut



To automatically create a shortcut to the report for use by Alliance 8300:

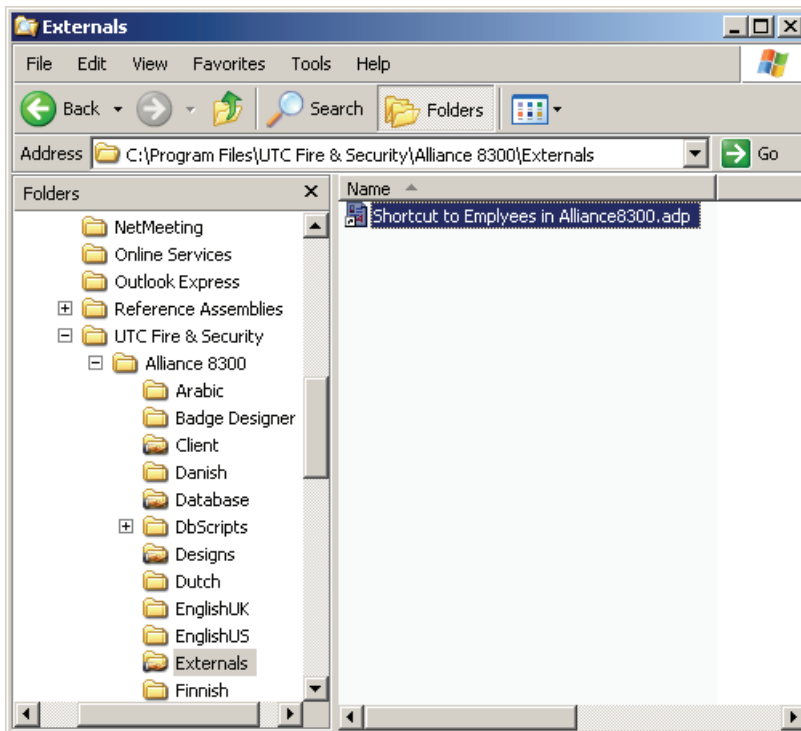
1. Open a Windows Explorer view of the Alliance 8300 Externals folder on the server computer.



Note: If you are creating the report from a client computer, navigate in Windows Explorer to the Server computer in Network Neighborhood to display the Externals folder.

2. Position Windows Explorer and MS Access on the Windows desktop so that both are visible.
3. Drag the report from the MS Access project to the Alliance 8300 Externals folder. See Figure 15 above.

Result: Windows automatically creates a shortcut to the MS Access report “Employees”.



This shortcut is accessible via the Alliance 8300 Reports > External Reports command (see “Launching External Reports from Alliance 8300” below).

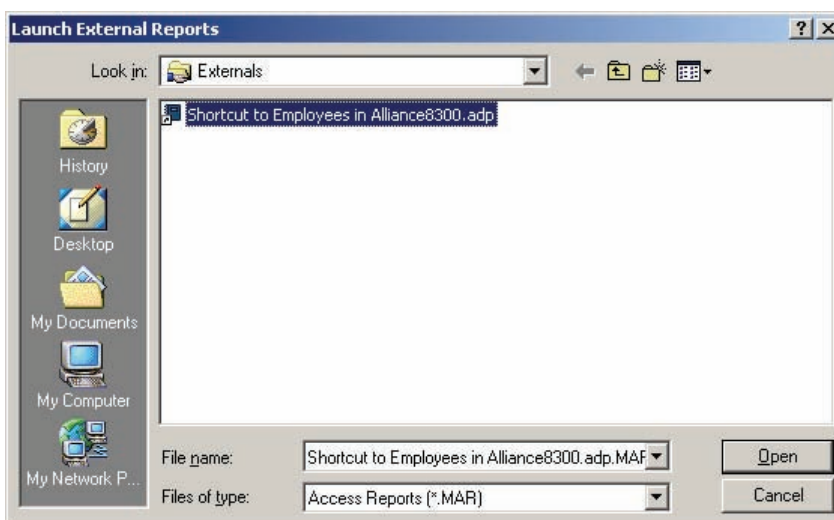
4. Close Microsoft Access and Windows Explorer when you are finished creating reports and dragging them into the Alliance 8300 Externals folder.

Launching External Reports from Alliance 8300

To run an Alliance 8300 external report:

1. In Alliance 8300, select Reports > External Reports.

Result: The Launch External Reports window displays the report shortcuts that you’ve dragged into the Externals folder on the server computer.



2. Select the required report and click Open. The database logon window displays.



3. Enter “exreport” as user name. Enter the password as setup using the maintenance application and then click OK.

Result: MS Access launches and opens the report in preview mode.

Note: MS Access is required on all client PCs that will run this report.

MS Access 2002 database utilities

Once you have created an MS Access project for each database, select Tools > Database Utilities > Compact and Repair Database. Refer to the online Microsoft Access Help for details of the Compact and Repair Database process.

Note: Do not select any other options from the Database Utilities menu unless instructed by a System Support technician.

Database and system management

This chapter discusses the various types of Alliance 8300 files, and the tools available for maintaining, backing up, and restoring these files.

Overview

The Alliance 8300 files stored on the server computer consists of the following types:

- Databases contained in the Alliance 8300/Database folder. See “Alliance 8300 databases” below for details.
- Application files and related data contained in the Alliance 8300 folder and its sub-folders (except for the Alliance 8300 databases in the Database sub-folder), and Windows System State data such as the Registry. See “Alliance 8300 files and settings” on page 101 for details.

The overall process of backing up Alliance 8300 is:

1. Run Alliance 8300/8700 Database Maintenance to backup the Alliance 8300 databases to create .BAK files. See “Backing up Alliance 8300 and 8700 databases” on page 100.
2. Run Microsoft Windows Backup to backup the entire Alliance 8300 folder (including the .BAK files created in step 1). See “Backing up with MS Windows Backup” on page 101.
3. Run Microsoft Windows Backup a second time to backup the Alliance 8300 Windows Registry settings. See “Backing up with MS Windows Backup” on page 101.

Alliance 8300 databases

The Alliance 8300 Professional server computer has three databases:

- Alliance8300: Contains configuration data for items such as operators, badges, and control panels.
- Alliance8300History: Contains current history data (data that has not been archived) including badge transactions and operator history.
- Alliance8300Archive: Contains transaction history data that was previously stored in the Alliance8300History database and automatically moved based the Alliance 8300 archive settings.

Maintenance operations for the Alliance 8300 databases include:

- Archiving: Archiving does not protect data against loss: it only moves data from the current database to the archive database for the purpose of maintaining system performance and for managing the use of hard disk space. See “Archiving Alliance 8300 history” on page 97.

- **Backing up:** Backing up is used to protect data against loss by enabling you to move the data to another location, and in a manner that allows lost data to be recovered. The Alliance 8300/8700 Database Maintenance utility is used to back up the Alliance 8300 databases. See “Backing up Alliance 8300 and 8700 databases” on page 100. If the Alliance 8700 Card Programmer is installed there will also be an Alliance8700CardProg database, which you will also need to back up.

Archiving Alliance 8300 history

The Alliance8300Archive database is created automatically by Alliance 8300 based on the archive period (daily, weekly, or monthly) defined in the Parameters form (see “Archive Database” on page 46, and Figure 11 on page 47). The default archive period is daily.

Alliance 8300 services must be running on the Alliance 8300 server for a scheduled archiving operation to occur. If the services are not running, Alliance 8300 attempts to perform the archiving operation the next time Alliance 8300 is started and a transaction is received.

Archiving appends the daily, weekly, or monthly data from the history database to the archive database, and removes this data from the history database.

Note: When the archive process runs, new data is appended to the current file. You must monitor the size of the Alliance8300ArchiveDAT database file to ensure that it remains below 2 GB in size and to ensure that the Alliance 8300 databases do not completely fill your hard drive. Depending on the use of archiving and diagnostic monitoring, you may need to reserve 20 GB of space free for use by Alliance 8300 (archiving can create very large temporary files).

The factors in determining whether the archive database is too large can be:

- The database must remain less than 2 GB in size
- The amount of available hard disk space on the Alliance 8300 server computer
- The performance you receive when running history reports
- The length of time you need to keep data
- Other factors specifically related to your installation

When you determine the archive database is too large:

1. Backup the data that you need to retain. See “Backing up Alliance 8300 and 8700 databases” on page 100.
2. Assuming that Alliance 8300/8700 Database Maintenance utility displayed a message verifying that the backup was successful, delete the data from the Alliance8300Archive database. See “Deleting Alliance 8300 archive history” on page 98.

Caution: If you do not back up the Alliance8300 Archive database, you will lose all the data stored in it.

After you perform the backup, validate the quality of the backup file, then label and store the media in a safe place.

Deleting Alliance 8300 archive history

To delete data from the archive database:

1. Start Alliance 8300 and login.
2. Select Administration > Parameters.
3. The Parameter form opens with the Settings tab displayed.

The screenshot shows the 'Parameter Form' window with the 'Settings' tab selected. The window has a title bar with standard Windows controls. Below the title bar is a tabbed interface with the following tabs: 'Settings', 'User Fields', 'Address Fields', 'Communication Settings', 'Clear Archive', and 'Badge learn'. The 'Settings' tab is active and contains several configuration sections:

- Archive Database:** Includes a section 'Select time interval to archive history:' with radio buttons for 'Daily' (selected), 'Weekly', and 'Monthly'. A dropdown menu shows 'Sunday'. Below this is an 'Archive now' button.
- Alarm activity printing:** Includes an 'Enable' checkbox (unchecked) and a 'Printer:' field with a 'Select Printer...' button.
- Console alarm sound:** Includes radio buttons for 'Continuous' and 'Short' (selected).
- Badge activity printing:** Includes an 'Enable' checkbox (unchecked) and a 'Printer:' field with a 'Select Printer...' button.
- Photo Aspect Ratio:** Includes 'Height' and 'Width' fields with numeric spinners. Height is set to 4 and Width is set to 3.
- Alarm Notifier E-mail Support:** Includes an 'Enable' checkbox (unchecked), an 'SMTP E-mail Server' dropdown, a 'To E-mail Address Field' dropdown, a 'From E-mail Address' text field, an 'E-mail User Name' text field, an 'E-mail Password' text field, a 'Confirm Password' text field, and a 'Send Test E-mail' button.

4. Select the Clear Archive tab.

Parameter Form

Settings User Fields Address Fields Communication Settings **Clear Archive** Badge learn

Earliest Date in Current Archive DB:

Latest Date in Current Archive DB:

Show date

Archive clean period

January 2011 January 2011

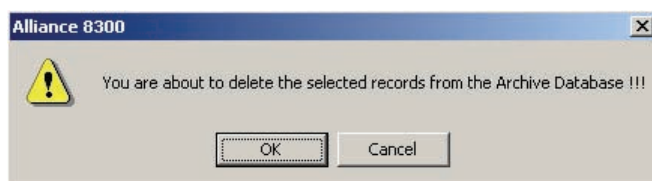
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

2011-01-21 2011-01-21

Start Date End Date

Delete

5. Click Show Date to display the Earliest Date in Archive DB and Latest Date in Archive DB fields in MM/DD/YYYY format. If you do not have any records in your archive database, the two date fields display No Record.
6. Choose the Start Date of the data that you want to remove from your archive database by selecting the month, then the day to begin your archive.
7. Choose the End Date of the data that you want to remove from your archive database by selecting the month, then the day to end your archive.
8. Click Delete. A confirmation message displays.



9. Click OK.

Result: The deletion of an archive database is taking place in the background. Background Tasks status is indicated on the status bar in the lower right side of the screen. The process may take hours to complete. The length of time is dependent on the size of the archive database and the hardware components of your computer.

Upon completion, a window displays the message: The data from the Alliance 8300 Archive database has been successfully deleted.

10. Click OK.

Backing up Alliance 8300 and 8700 databases

The Alliance 8300/8700 Database Maintenance utility is used to back up the Alliance 8300 and Alliance 8700 databases to .BAK files, which can then be backed up using Microsoft Windows Backup. See “Backing up with MS Windows Backup” on page 101.

To back up the database files:

1. Create a folder on your system or any where on the network using a mapped drive where the backup files will be stored.
2. Run the Alliance 8300/8700 Database Maintenance utility on the Alliance 8300 server from Start > Programs > UTC Fire & Security > Alliance 8300.
3. The Alliance 8300/8700 Database Maintenance window displays.
4. Click Backup.
5. The Backup window displays.

The screenshot shows a 'Backup' dialog box. It has a title bar with 'Backup' and a close button. The main area is divided into two sections. The top section is labeled 'Backup Destination' and contains the following fields: 'Login:' with a text box containing 'sa', 'Password:' with an empty text box, 'Alliance:' with an empty text box and a check box to its right, 'Alliance Archive:' with an empty text box and a check box to its right, 'Alliance History:' with an empty text box and a check box to its right, and 'Alliance Card Programmer:' with an empty text box and a check box to its right. To the right of the 'Alliance', 'Alliance Archive', and 'Alliance Card Programmer' fields are 'Browse' buttons. At the bottom center is a 'Backup' button.

6. Type the “sa” login and password.

7. Click Browse to choose, where the backup files will be stored.

Result: The .BAK files in each field will be named automatically, to include the directory path, file name, date, and time.

8. If you choose not to back up any of the three databases, clear the check box at the end of that field. If the check box is selected but no destination is entered in the database field, backup of that database file will not occur.

9. Click Backup.

Result: The backup process begins. When backup is complete, a dialog box displays a message verifying the successful backup of the chosen databases.

10. Click OK.

11. Exit the Maintenance window.

Alliance 8300 files and settings

Alliance 8300's application files and related data are contained in:

- The Alliance 8300 folder and its sub-folders (except for the Alliance 8300 databases in the Database sub-folder).
- Windows System State data (including Windows Registry settings).

Backing up is used to protect data against loss by enabling you to move the data to another location, and in a manner that allows lost data to be recovered.

Windows Registry settings may be backed up using the following methods:

- Use Microsoft Windows Backup. See "Backing up with MS Windows Backup" below.
- Use Windows Registry Editor (regedit) to export the Windows Registry (or a portion of it) to a text file. See Registry Editor on-line help for details.

Note: Performing backup operations during busy periods may reduce the performance of the Alliance 8300 system.

You can use any backup program or media such as tape, zip disk, CD, or a network folder to produce a backup copy of selected data. The size of the files in the folder you want to back up will be a determining factor of which media to use.

If you have the Alliance 8300 Imaging option installed, the following additional folders will be stored in the Alliance 8300 folder:

- Images: Will only need to be backed up if you have Imaging installed. Contains the picture files of badge holders.
- Signatures: Will only need to be backed up if you have Imaging installed. Contains the signature files of badge holders.
- Graphics: Will only need to be backed up if you are using Alarm Graphics. Contains the alarm graphics maps.
- Designs: Will only need to be backed up if you have Imaging installed and previously created badge designs in the folder.

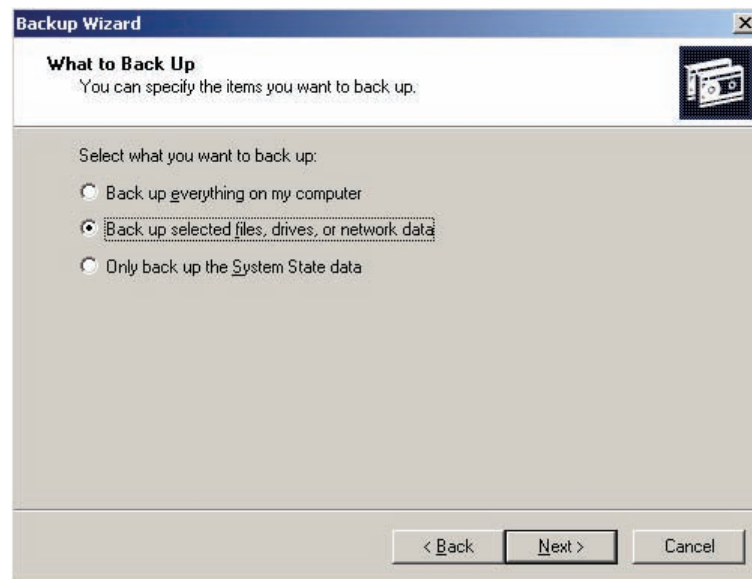
Backing up with MS Windows Backup

Microsoft Windows Backup enables you to backup:

- Files and folders
- Windows System State data (including Windows Registry settings)

To backup both of these types of data, you would run Microsoft Windows Backup twice, selecting different options (see Figure 16 on page 102).

Figure 16: Using the Backup Wizard to select either files or system state data



If you use a tape drive for backup, typical instructions for using a tape drive are listed below. Similar procedures apply for using Microsoft Windows Backup to backup to other media.

To back up to the tape drive:

1. Insert the tape to which you want to back up.
2. Click on Start > Programs > Accessories > System Tools, then Backup.
Result: Microsoft Windows Backup will appear.
3. From the Welcome to the Backup and Recovery Tools window, click Backup Wizard, then Next.
See Figure 16 above.
4. Assuming you want to backup files, navigate to C: \Program Files\UTC Fire & Security\Alliance 8300 or wherever the installation of Alliance 8300 resides on your computer. Select the folder to back up. Click Next.

Result: The Where to Store the Backup window displays.

Note: Microsoft Windows Backup does not backup the Alliance 8300 databases in the Database sub-folder. These must first be backed up using the Alliance 8300/8700 Database Maintenance utility, and then the resulting .BAK files can be backed up using Microsoft Windows Backup. See “Backing up Alliance 8300 and 8700 databases” on page 100 for details about backing up these files.

5. Select the Backup media type and Backup media or file name and click Next.
6. Completing the Backup Wizard window displays.
7. Click Finish.

Result: The Backup Progress displays.

8. Click Close and exit the Backup window.

Backing up to your computer CD-RW drive

If you use a CD-RW drive for backup, typical instructions for using a CD-RW drive are listed below (Adaptec Easy CD Creator 4 is only an example).

To back up to the CD-RW drive:

1. Insert the blank CD to which you want to back up.
2. Click on Start, Programs, Adaptec Easy CD Creator 4, then Create CD.
Result: The Easy CD Creator 4 Welcome window displays.
3. From the Welcome window, click Data, then Data CD.
4. In the Easy CD Creator explorer window, navigate to the Alliance 8300 folder, then select the folder or folders to back up.

Note: Your Alliance 8300 database folder contains files with .mdf and .ldf extensions. DO NOT COPY, BACK UP, OR EDIT THESE FILES. See “Backing up Alliance 8300 and 8700 databases” on page 100 for details about backing up these files.

5. Drag and drop the files to the CD Layout window. This enables the Create CD icon on the main menu bar.
6. Click Create CD from the main menu.

Result: The CD Creation Setup window displays.

7. Select your Target Device from the drop-down list and click OK.

Result: A CD Creation Process window displays the progress of the creation procedure.

8. When a completion message displays in the progress window, the CD creation process is complete. Click OK to exit the CD Creation Process window.

9. From the File menu, select Exit to close the Easy CD Creator 4 application.

Restoring data from a backup

You may need to restore data from a backup for a variety of reasons:

- To verify that a backup was successful
- To establish backup and restore procedures
- To recover lost data (accidental deletion or system failure)
- To recover a deleted archive database so that reports can be run using the data

Restoring Alliance 8300 and 8700 databases

Note: The backup files must be moved to the destination computer. The Alliance 8300/8700 Database Maintenance utility can only restore from a local machine (in this case the Alliance 8300 server).

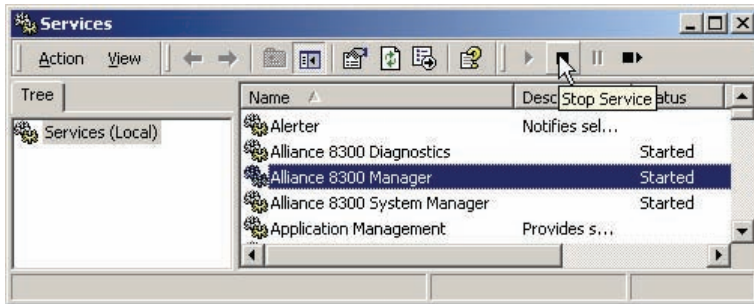
To restore an Alliance 8300 database backup:

1. Stop the Alliance 8300 services. Select Start > Settings > Control panel. Double-click Administrative Tools and then double-click Services.

Alternatively, select Start > Run and enter services.msc. Click OK.

Result: The Services window displays.

2. Find the Alliance 8300 services and stop them in the following order: Alliance 8300 Manager, Alliance 8300 System Manager, Alliance 8300 Diagnostics.

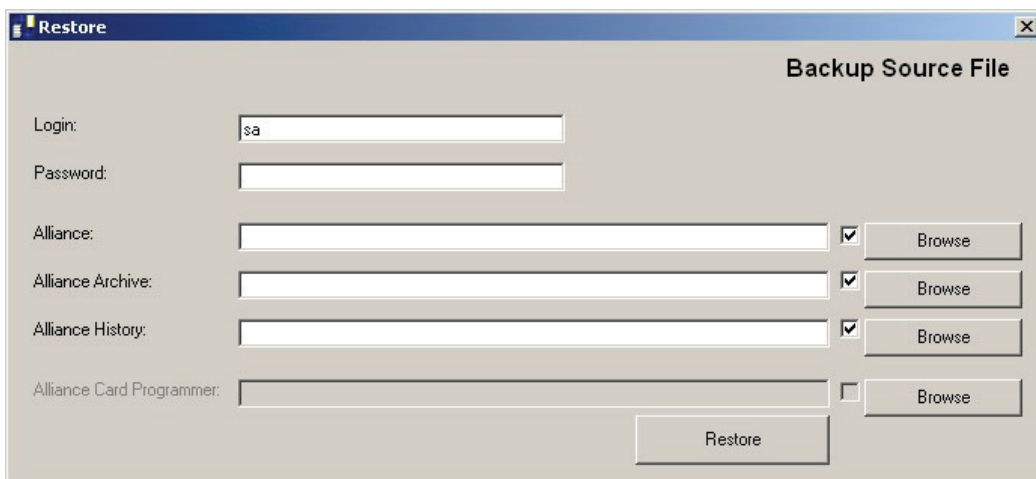


3. If you are using MS SQL Server 2008 R2 Workgroup, Standard, or Enterprise Edition, restore the contents of the Images, Signatures, Graphics, and Designs folders from your backup media to the appropriate Alliance 8300 subfolders. See "Restoring files" on page 105.
4. Run the Alliance 8300/8700 Database Maintenance utility on the Alliance 8300 server from Start > Programs > UTC Fire & Security > Alliance 8300.

Result: The Alliance 8300/8700 Database Maintenance window displays.

5. Click Restore.

Result: The Restore window displays.



6. Type the sa login and password.
7. Click Browse to choose the Alliance database backup file. The program will then try to find all other backup files in this folder.

8. If you choose not to restore any of the three databases, clear the check box at the end of that field. If the check box is checked, but no destination is entered, the restoration will not occur.

9. Click Restore.

Result: The restoration process begins. When restoration is complete, a dialog box displays a message, verifying the restoration of the chosen databases.

Note: When you restore a database, you need to re-license Alliance 8300 and all clients connected to it.

10. Click OK.

11. Exit the Alliance8300 Database Maintenance utility.

12. Re-register the Alliance 8300 License using the license key initially provided. (If Alliance 8300 does not accept the original license key, follow the complete license registration procedure described in the Alliance 8300 Installation Guide.)

Result: The database restoration is complete and your Alliance 8300 application is ready to start.

Restoring files

If you used the Backup Wizard in Microsoft Windows Backup to backup your files (see “Backing up with MS Windows Backup” on page 101), then you can use Restore Wizard to restore your files.

Note: If you need to restore backed-up files from the Alliance 8300 sub-folders, restore the files and not the entire folder because the folder will not have the original share property as the original. Alliance 8300 depends on some folders being shared and having specific share properties.

System recovery

If your Alliance 8300 Professional System server computer experiences severe errors while operating, you might need to rebuild the system and restore your databases. Follow the sequence of steps listed to recover your system.

The checklist below assists you in recovering your Alliance 8300 Professional system. Complete the steps in the order they appear:

- ☐ Repeat all the steps in the Alliance 8300 Installation Guide from Preparing The Operating System to the end of Installation Part 1.
- ☐ Restore the contents of the Images, Signatures, Graphics, and Designs folders from your backup media to the appropriate Alliance 8300 subfolders. See “Restoring files” above.
- ☐ Use the Alliance 8300/8700 Database Maintenance utility to restore the three Alliance 8300 databases and the Alliance 8700 Card Programmer database (if applicable) from your backup media. See “Restoring Alliance 8300 and 8700 databases” on page 103.

- ❑ Re-register the Alliance 8300 License using the license key initially provided (if Alliance 8300 does not accept the original license key, follow the complete license registration procedure described in the *Alliance 8300 Installation Manual*).
- ❑ Restart the computer.

Diagnostics and troubleshooting

Alliance 8300 provides an extensive diagnostic utility named DiagView. To access DiagView, select Administration > Diagnostic Viewer. This utility is very flexible in that you can selectively activate the monitoring of Alliance 8300 system components when needed.

Note: Due to this, the amount of data stored for diagnostics may make finding issues difficult. Activate diagnostics only when requested so be qualified support engineers.

This utility plus some common questions and answers are covered in this chapter.

Turning on diagnostics

By default only a limited number of debug messages are stored and displayed. To store or display more debug messages in the Diagnostics Log within Alliance 8300, the diagnostics for that component you wish to monitor (COM port, control panel, or client) **MUST** be turned on.

Each client computer will have a set of diagnostic objects that represent what can be monitored on that machine. Diagnostic objects can be controlled remotely (turned on or off). All diagnostic objects can write messages to a common logfile or any diagnostic object can write to a separate logfile that can be defined by the user.

Creating a Logfile

To create a logfile:

1. Select Administration > Logfile.
Result: The Logfile form displays.
2. Click Add Record.
3. Your Computer name displays.
4. Enter a LogFile name to include an .spl extension.
5. Click Browse to navigate and select a folder in which to store the logfile.
6. Click Save.

To enable diagnostics:

1. Select Administration > Diagnostic Setting.
2. Click Search in the toolbar to display a list of components that you can monitor.
3. Select the desired component.

Note: All diagnostic objects are prefixed with a machine name.

4. Select Enable debug messages check box and click Save.
5. When you are finished troubleshooting the system, don't forget to go back and DISABLE debug messages.

Caution: The more items you turn on for monitoring, the more the Alliance 8300 system performance is compromised! This is even more important when monitoring port, communications, or control panel items.

There are many components available to monitor.

- The diagnostic objects, such as COM1, display the communications protocol between the control panel and its server as the information comes into the COM port.
- The diagnostic objects, such as control panel 1, display how information is being processed for that control panel.
- The remaining components are for client, manager service, system service, and other functional components.

Viewing the diagnostics logs

Alliance 8300 provides a convenient way to view what's happening on the system. For each client, there is a default logfile (others can be created) for each day of the week such as A8K3THURSDAY.SPL.

Additionally, for each client, there is a log located in the `WINNT\system32` folder. Under normal system operation, this log will not be used. It will be used to log messages when the database cannot be reached.

During normal operation of Alliance 8300, information as well as debug messages are written to the daily log file. Under abnormal conditions, the log file may also contain warning and/or fatal messages.

Alliance 8300 has a log file viewer named DiagView, which can be used to open log files and display logged events in real time. To access DiagView, select Administration > Diagnostic Viewer or alternatively select Start > Programs > UTC Fire & Security > Alliance 8300 > Diagnostic Viewer. Every time Alliance 8300 writes an entry to the log file, DiagView displays the latest message. By default, DiagView displays only the latest 1000 messages. The number displayed can be changed in DiagView via the File > Preferences command.

All log files should be saved in the logs folder; it will be easier to locate for backups and upgrades. It is a shared folder, which means other clients can gain access to the log files.

Questions and answers

This section provides answers to some common questions.

Caution: Always use extreme care when editing the Windows registry! Making a mistake while editing the registry can cause Windows to behave erratically. To fix this problem, you will need to reinstall your operating system.

Installing Alliance 8300

What is the order of events during installation?

The complete order of installation is detailed in the *Alliance 8300 Installation Manual*. A summary of the installation process follows.

To install the program:

1. Install Alliance 8300 on your Server computer (license domain and database server run on the Server computer).
2. Create the database on the server.
3. Register the Alliance 8300 license on the Server computer.
4. Start the Alliance 8300 application.
5. Use the Client form to add and configure all your clients.
6. Install Alliance 8300 on your client computers.
7. License the client on the Alliance Server.

What does this message mean: “You must have Administrator Rights in order to install Alliance 8300 Server software”?

You are logged in to Windows as a user who does not belong to the local Administrators group. The Alliance 8300 software can only be installed by a Windows user who belongs to the local Administrators group.

Solution: Log out, then log in as a Windows user who belongs to the Administrators group or add the Windows user to the Administrators group.

Starting Alliance 8300

The Alliance 8300 server computer must be set up in a manner that the Alliance 8300 services start up automatically each time the server computer starts up. The Alliance 8300 services, running on the Alliance 8300 server computer, enable Alliance 8300 to run on remote Alliance 8300 client computers. During installation of the Alliance 8300 server, the required Alliance 8300 services are set to start automatically.

The process of setting up Alliance 8300 services to start automatically is described in the *Alliance 8300 Installation Manual*.

Alliance 8300 will not be able to run on a remote Alliance 8300 client computer in any of the following circumstances:

- If the Alliance 8300 server computer is not running.
- If the Alliance 8300 services are not running on the Alliance 8300 server computer. See “Restoring Alliance 8300 and 8700 databases” on page 103 for an example of running services (indicated by “Started” in the Status column).
- If the remote Alliance 8300 client computer cannot communicate with the Alliance 8300 server computer over the network because of network problems.
- If the password for the secure windows account on the client does not match the password setup for the secure windows account on the Alliance 8300 server.
- If the Windows login used on the remote client computer cannot access the Alliance 8300 shared folders on the server computer. To check this, log into Windows on the remote client computer as user ‘secure’ with the assigned password, and attempt to restart Alliance 8300 on the remote client computer.
- If the Alliance 8300 client record (Administration > Client) for the remote Alliance 8300 client computer has not been set up in the Alliance 8300 server computer.
- If the maximum number of clients permitted by the Alliance 8300 license is currently being used. On the Alliance 8300 server computer, check the bottom of the Client Monitor form and verify that there is at least one license available.
- If Alliance 8300 was not correctly installed on the remote Alliance 8300 client computer (for example, if the wrong Alliance 8300 server name was used during the client installation, or if the Alliance 8300 client wasn’t licensed correctly).

I get a connection error when I try to start Alliance 8300 on a remote client computer

To fix this problem:

1. Make sure the Alliance 8300 server computer is running and connected to the network.
2. On the Alliance 8300 server computer, go to the Services form and check Alliance 8300 services. If the Status column is blank for a service, then it is not running. Highlight the service, and click the Start button:
 - If the status changes to Started, then the service is now running. Try to start Alliance 8300 on the remote computer now.
 - If the status does not change to Started, use DiagView on the server computer to check the current day’s log. It should display an error message providing a reason for shutting down.

3. On the Alliance 8300 server computer, ensure that the Alliance 8300 client record (Administration > Client) for the remote Alliance 8300 client computer has been set up.
4. On the Alliance 8300 server computer, check the bottom of the Client Monitor form and verify that there is at least one license available for the client to use.
5. On the Alliance 8300 client computer, verify that the currently logged in Windows user name and password has been set up by the network administrator with domain permissions to access the Alliance 8300 shared folders on the server computer. The network administrator must use the utilities described in "System administration utilities" on page 139 to set up users and groups.
6. Verify that you are using TCP/IP as your network protocol, which it is configured properly, and is used on both the client and server computers. Verify if firewalls and routers do not prevent connection between Alliance clients and server.

What are some of the reasons the Alliance 8300 System Manager Service will not start?

Possible causes include:

- Computer hardware has failed
- Computer hardware has been replaced
- The service cannot access the database
- The client machine name is not in the client table
- The services on the database server are not running

Solution: Alliance 8300 licensing uses the server computer's hardware configuration (among other things) when it generates the machine seed key, which is used for licensing. A change in hardware may require Alliance 8300 to be relicensed.

What are some of the reasons the Alliance 8300 Manager Service will not start?

Possible causes include:

- Computer hardware has failed
- Computer hardware has been replaced
- System service on the local machine will not start
- The local machine did not receive a ping from the license domain machine within the ping timeout interval (check the license domain services are running)
- Client license count may have been exceeded

Solution: Alliance 8300 licensing uses the server computer's hardware configuration (among other things) when it generates the machine seed key, which is used for licensing. A change in hardware may require Alliance 8300 to be relicensed.

My services shut down unexpectedly. The log reports that the message database is down.

This indicates a problem with connectivity to the database. In order not to lose any transactions, Alliance 8300 will save all badge and alarm messages by writing them to a file and read the file back in when the services start up again.

Solution: Correct the connectivity problem with the database and restart services.

What does this message mean: “Maximum Number of Clients Limit Reached”?

The maximum number of clients permitted by the Alliance 8300 license is already connected to the server.

You may need to purchase additional Alliance 8300 client licenses from UTC.

What does this message mean: “Simple File Sharing is not compatible with the application”?

Alliance 8300 requires Classic model of the file sharing in the system.

See “Appendix D. Configuring file sharing” on page 129.

What does this message mean: “No security packages are installed on the machine, or the user is not logged on, or there are no compatible security packages between the client and server”?

Communications may be blocked by DCOM Services permissions or by a firewall (in the case of Windows XP SP2), or windows accounts and related access rights do not match on all PC's running Alliance.

Solution: Check if on all PC's running Alliance windows accounts for all operators are available with the same password and are assigned to the windows group AllianceGroup. Use the SplnitClient utility (see “SplnitClient.exe” on page 140) to configure other DCOM related items for the client computers and then restart the Alliance 8300 services.

More than one client computer may be involved. The client displaying the error message (affected client) may be unable to connect to a panel, which is hosted by a different client (host).

After using the SplnitClient utility on both client computers, restart the services on the host before restarting the services on the affected client.

Using Alliance 8300

Can I customize the toolbar and add more buttons?

No. The toolbar cannot be customized and buttons cannot be added to the toolbar.

You can, however, change the position of the toolbar. Simply click and drag the toolbar wherever you would like it to be on the screen.

How do I perform a search on a specific item?

The Search button can be found on any form that provides search capabilities. If you click on this button and the current form is blank, all records will be returned. To specify criteria, simply fill in the desired information. For example, if you want to find all badgeholders with the last name Smith, type Smith in the Last name field and click on the Search button.



You can also use the * character which allows you to search for patterns. For example, to search for badgeholders with the last name starting with Sm* would yield such names as Smith and Smithers. Searching for *th would give names like Smith, not Smithers. Searching for *ith* would find both Smith and Smithers.

Why can't I delete a record?

Some forms, such as the Door/Output Status form and the Door/Output Control form, do not contain a Delete button because they display status information only.

Other forms, such as the Alarm form or Alarm Category also do not contain a Delete button. To keep the system stable, NO ONE is given permission to delete these records, not even a System Administrator. These records are deleted when the associated control panel is deleted. However, on all other forms, you may be assigned the permission action All. (Permission actions are assigned using the Permission form. Verify that the permission assigned to the operator on the Operator form contains the desired permission actions by checking that permission on the Permission form.) If you can't delete on those forms, you do not have permission to do so.

Why are there no alarms being displayed on the Alarm Monitor form?

Go to the Alarm form and click on the Alarm tab. Make sure that the Monitor option is enabled and the alarms belong to your facility.

How do I get into the Badge Design program?

1. First, you must have the Alliance 8300 Imaging installed. Refer to your Alliance 8300 Installation Manual for more information on installing this package.
2. Second, the Alliance 8300 client you are using must have a license for Imaging. Select Operations > Client Monitor. The bottom section of the Client Monitor form contains the section Imaging Information. (You may need to make the window larger to display the number of Imaging licenses presently in use and the number of Imaging licenses you are allowed, as purchased with your system.) Locate the name of your computer in the Client list. Then, look in the column Imaging status and verify that it reads Enabled.

If Imaging status reads Disabled and the numbers indicate a license is available for use, select Administration > Client. On the Client form, Client tab, select Enabled in Imaging Status to enable Imaging. Return to the Client Monitor form to check the Enabled status.

3. If you have the Alliance 8300 Imaging installed and your client has a license, you will need a badge design file. You should create your own and then save it in your Alliance 8300 Designs folder. The Edit Badge Design button becomes enabled allowing you to enter the Badge Design program.

When I run DiagView and try to open a file, only one logfile shows in the Logfile Dialog.

Solution: This indicates the database cannot be accessed. Test the database connection.

Services shut down while DiagView is running. A dialog box pops up and displays the message “Diagnostic Manager Service has Shutdown”. After I restart services, no new messages are displayed.

Solution: Communication has been lost with the services and the file needs to be reopened again when the services are up and running (refer to Table 5 below).

I do not understand the order in which the services should be shut down and started.

Shutting down the Diagnostics Service will shut down the other Services. Note the service dependencies as described in Table 5 below.

Table 5: Service Dependencies

Service	Dependency
Alliance 8300 Diagnostics	MS SQL
Alliance 8300 System Manager	Diagnostics
Alliance 8300 Manager	Diagnostics, System Manager

I shut down my license domain server (cold boot). My clients are reporting database errors (that is, they have lost their network connection).

This can occur when the network goes down for any purpose (common examples: hub loses power temporarily; network cable cut or broken).

Solution: It is best to either have clients use the Client Monitor form to force users off, or notify all clients to restart after a cold boot of the server is complete and after services have restarted on the license domain.

My services will not shut down from the Services window. Is there something I can do besides rebooting the system?

Solution: Run the utility SPStop.exe found in the Alliance 8300 folder. See “SPStop.exe” on page 144.

What should a normal startup of services look like in the logfile?

It should look similar to the following with the exception of machine name and machine-encoded seed and control panels that may show up in the log. The following sample startup script displays a sequence of key events in the startup

process. Note SYSTEM SERVICE STARTED, STARTING MANAGER SERVICE, etc.

Figure 17: Sample Services Startup

Date	Time	Module	Message
11/20/07	10:08:26	A8K3 Diagnostic	Attempting to Destroy the Machine Manager
11/20/07	10:08:26	A8K3 Diagnostic	Machine Manager Destroyed
11/20/07	10:08:26	A8K3 Diagnostic	System Manager Destroyed
11/20/07	10:08:26	A8K3 Diagnostic	Attempting To Destroy License Handler
11/20/07	10:08:26	A8K3 Diagnostic	License Handler Destroyed
11/20/07	10:08:26	A8K3 Diagnostic	Attempting To Destroy Ping Handler
11/20/07	10:08:26	A8K3 Diagnostic	Ping Handler Destroyed
11/20/07	10:08:28	A8K3 Diagnostic	Process Terminator Destroyed
11/20/07	10:08:28	A8K3 Diagnostic	***** SYSTEM SERVICE HAS STOPPED! *****
11/27/07	08:33:03	A8K3 Diagnostic	Query did not find the desired record for ClientName =
11/27/07	08:33:03	A8K3 Diagnostic	Using A8K3 Diagnostic
11/27/07	08:33:03	A8K3 Diagnostic	***** STARTING SYSTEM SERVICE *****
11/27/07	08:33:04	A8K3 Diagnostic	Ping Handler Initialized
11/27/07	08:33:05	A8K3 Diagnostic	License Handler Initialized
11/27/07	08:33:05	A8K3 Diagnostic	System Manager Initialized
11/27/07	08:33:05	A8K3 Diagnostic	Machine Manager Initialized
11/27/07	08:33:05	A8K3 Diagnostic	Process Terminator Created
11/27/07	08:33:05	A8K3 Diagnostic	***** SYSTEM SERVICE STARTED *****
11/27/07	09:33:32	A8K3 Diagnostic	Query did not find the desired record for ClientName =
11/27/07	09:33:32	A8K3 Diagnostic	Using A8K3 Diagnostic
11/27/07	09:33:32	A8K3 Diagnostic	***** STARTING SYSTEM SERVICE *****
11/27/07	09:33:32	A8K3 Diagnostic	Ping Handler Initialized
11/27/07	09:33:33	A8K3 Diagnostic	License Handler Initialized
11/27/07	09:33:33	A8K3 Diagnostic	System Manager Initialized
11/27/07	09:33:33	A8K3 Diagnostic	Machine Manager Initialized
11/27/07	09:33:33	A8K3 Diagnostic	Process Terminator Created
11/27/07	09:33:33	A8K3 Diagnostic	***** SYSTEM SERVICE STARTED *****

Hardware

My COM port is not working as expected. What should I do now?

Use the Controller Utility form to troubleshoot communications between the host and the control panel.

- Make sure the State field shows the control panel as Online. If it is Offline, right-click then select Set Online. If it is Error, then the host is not able to communicate correctly with the control panel.
- Make sure the Connection field shows Connected.
- Make sure the baud rate setting for the computer's COM port is 4800 for Advisor Master control panels or matches the setting in the FAS device (Global repeater or panel) connected to the COM port.
- Make sure the Comm. Port field shows the proper communications port for this control panel, that is, COM1 for COM port 1.

Check the Status field to check the condition of the communications (status messages are Idle or Normal).

If everything looks OK on the Controller Utility form, check the hardware settings:

1. Click Start, Settings, and then Control panel.
2. From the Control panel window, double-click System, then select Device Manager, then Ports.
3. Check that the baud rate setting for the computer's COM port matches the setting for the COM port in Alliance.

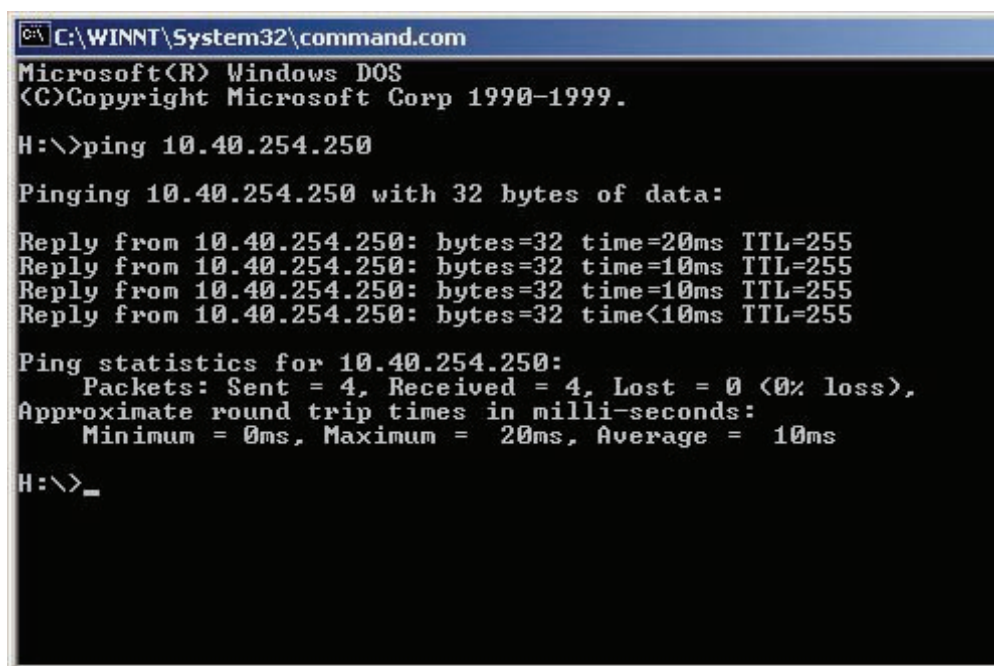
My network control panel is not working as expected. What should I do now?

Follow the same steps as in COM Port Not Working (as discussed above). Verify the control panel's IP address from the devices Communications section. If no problems are identified on the Controller Utility form, try pinging the control panel using the IP address shown in the Controller Utility form.

For example: C: \ping 10.40.254.250

If the ping command fails with a Request timed out message, verify that the host IP address is correct, that the host is operational, and that all the gateways (routers) between this computer and the host are operational. You should receive a reply screen display, similar to the shown on Figure 18 below.

Figure 18: Sample Ping command reply screen



```
C:\WINNT\System32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-1999.

H:\>ping 10.40.254.250

Pinging 10.40.254.250 with 32 bytes of data:

Reply from 10.40.254.250: bytes=32 time=20ms TTL=255
Reply from 10.40.254.250: bytes=32 time=10ms TTL=255
Reply from 10.40.254.250: bytes=32 time=10ms TTL=255
Reply from 10.40.254.250: bytes=32 time<10ms TTL=255

Ping statistics for 10.40.254.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 20ms, Average = 10ms

H:\>_
```

Server-client communications

A client computer is not able to control a panel remotely

Solution: Communications may be blocked by DCOM Services permissions or by a firewall (in the case of Windows XP SP2). Use the SplnitClient utility (see

“SplnitClient.exe” on page 140) to configure these items for the client computers and then restart the Alliance 8300 services.

More than one client computer may be involved. The client displaying the error message (affected client) may be unable to connect to a panel, which is hosted by a different client (host).

After using the SplnitClient utility on both client computers, restart the services on the host before restarting the services on the affected client.

Client’s connection to the license server is lost

When the connection to the license server is lost, Alliance behaves as if it reaches all license-related limits excluding the license time: the “License Unavailable” mode with 12 hours timer is activated. If the connection to the license server is restored before this time expires, Alliance returns to the fully operational mode; otherwise the Alliance services are shutdown.

Uninstalling Alliance 8300

Refer to the *Alliance 8300 Installation Manual* for details.

Appendix A. CCTV Support

Introduction

Alliance 8300 interfaces with CCTV (Closed Circuit Television) systems. The systems are CCTV control systems that operate separately from Alliance 8300 and require their own hardware and software provided by the CCTV manufacturer. The interface between the CCTV system and Alliance 8300 provides the capability to automatically control CCTV cameras based on alarms within Alliance 8300.

Setup and configuration

For the physical setup of the CCTV system that you purchased, refer to the documentation you received with the CCTV system.

Sources of additional details include the following:

- Alliance 8300 CCTV Interface Guide covers setup and configuration of the CCTV system with Alliance 8300.
- Alliance 8300 Online Help contains additional information on setting up CCTV alarms.

Digital Video Recorders (DVRs)

Alliance 8300 has the ability to integrate with UTC Fire & Security digital video recorders.

Using your Alliance 8300 system, you are able to set up, control, search, and view live and recorded video directly from your computer. Refer to the *Alliance 8300 CCTV Interface Guide* for detailed instructions to setup and configure a DVR system with Alliance 8300.

Appendix B. Changing the server name

Introduction

The Alliance 8300 Server computer holds the Alliance 8300 databases, controls communications with Alliance 8300 client computers, and controls the Alliance 8300 licensing.

The need may arise to change the name of the Alliance 8300 Server computer. This could typically be due to upgrading the computer or moving the Alliance 8300 Server to a different computer (i.e. installing Alliance 8300, and restoring the Alliance 8300 databases, to a computer with a different name than the original server's computer name).

Tip: If you need to move Alliance 8300 Server onto a new computer, you may save time by changing the new server's computer name to be the same as the old server's computer name before installing Alliance 8300 and restoring the Alliance 8300 databases. However, after installing Alliance 8300 you would still need to re-license the new server and all the clients.

If you have already installed Alliance 8300 on the new server computer and you need to change the server's computer name, you must change it in four places:

- On the Windows operating system, Network Identification tab of your System Properties. See "Changing the name in Windows" below.
- In the Alliance 8300 registry setting. See "Changing the name in Windows registry" on page 120.
- In the Alliance 8300 database. See "Changing the name in the Alliance 8300 database" on page 121.
- In the ODBC Data Source Administrator. See "Changing the name in ODBC" on page 121.

Note: Any Alliance 8300 computer (server or client) that has had its computer name changed will lose communication with all controllers (control panels) hosted by that computer. In such a case, the Controller records for affected panels would have to be deleted and then recreated using the new computer name.

Changing the name in Windows

To change the name of the server computer in Windows:

1. Right click the My Computer icon on your desktop.
2. Select Properties from the context menu.
3. Select the Network Identification tab from the System Properties.
4. Click Properties.

Result: The Identification Changes screen displays your Computer Name. Enter the new name of the Server computer. It should consist of a maximum of 15 alphanumeric characters with no spaces.

5. Click OK, then Apply. You will be asked to reboot your computer. Select OK.
6. When the computer reboots, you may receive an error message from MS SQL. Click OK to close the dialog. This error will be addressed later, as you change the server computer name in MS SQL.

Changing the name in Windows registry

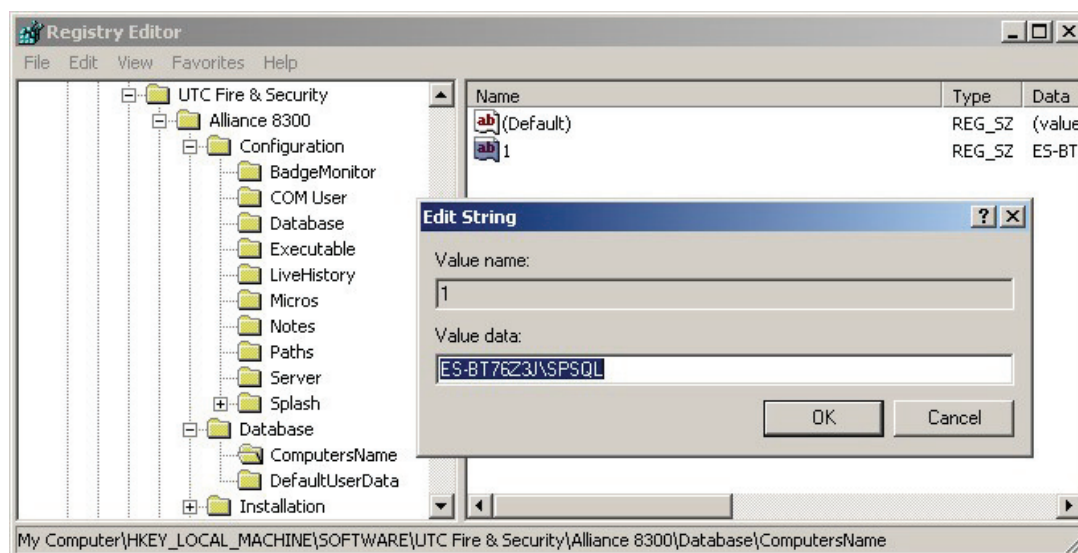
To change the Alliance 8300 Windows registry entry for the computer name:

1. Shut down the Alliance 8300 client application.
2. Stop Alliance 8300 services.
3. Click Start, then Run, type regedit and then click OK.

Caution: Using the Registry Editor incorrectly can cause serious problems that may require you to re-install your operating system. Neither UTC nor Microsoft guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk!

4. Open the following by clicking “+” in front of HKEY_LOCAL_MACHINE, then SOFTWARE, UTC Fire & Security, Alliance 8300, Database, then ComputersName.
5. On the right side of your screen, double click the key name 1 to open the Edit String dialog box.

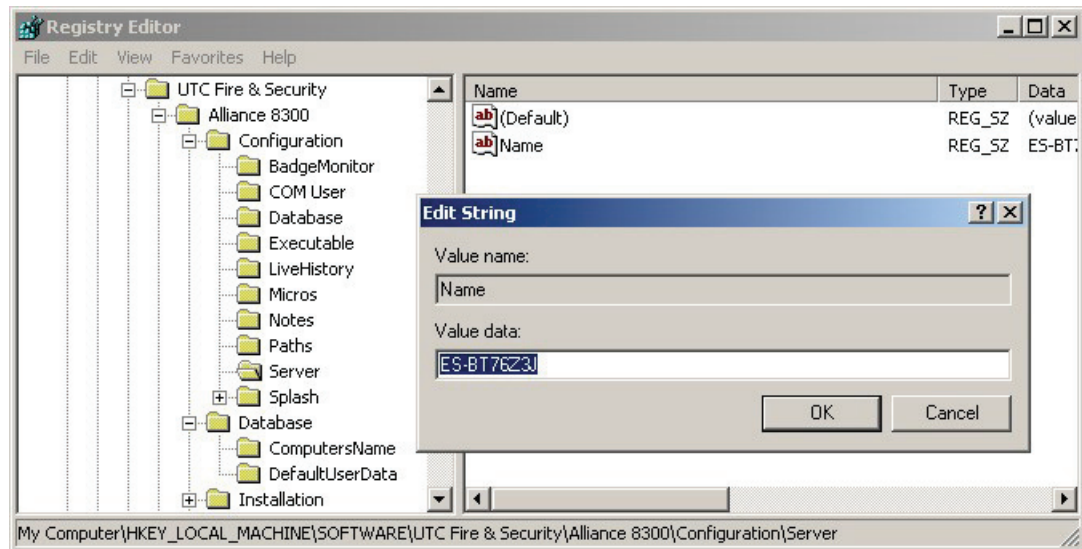
Result: The screen that displays should be similar to the following:



6. Type the new server name in front of \SPSQL, and then click OK.
7. Open the following by clicking “+” in front of HKEY_LOCAL_MACHINE, then SOFTWARE, UTC Fire & Security, Alliance 8300, Configuration, then Server.

8. On the right side of your screen, double click the key name Name to open the Edit String dialog box.

Result: The screen that displays should be similar to the following:



9. Type the new server name in front of \SPSQL, and then click OK.
10. Select Registry > Exit to close the Registry Editor.

Changing the name in the Alliance 8300 database

Use the SPInitClient utility to update the server and client computers when the Alliance 8300 server computer has its name changed or is moved to a different computer.

Refer to "Changing the server name" on page 140 for details.

Changing the name in ODBC

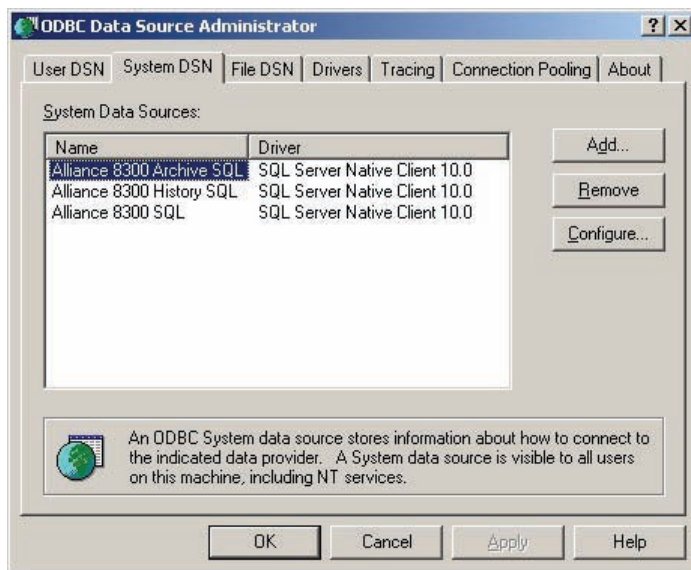
Open Database Connectivity (ODBC) is used to enable Alliance 8300 (on the server and on clients) to connect with the Alliance 8300 databases on the server computer.

If the name of the server computer is changed, then the new name must be applied to the Alliance 8300 ODBC system data sources for the server and all client computers.

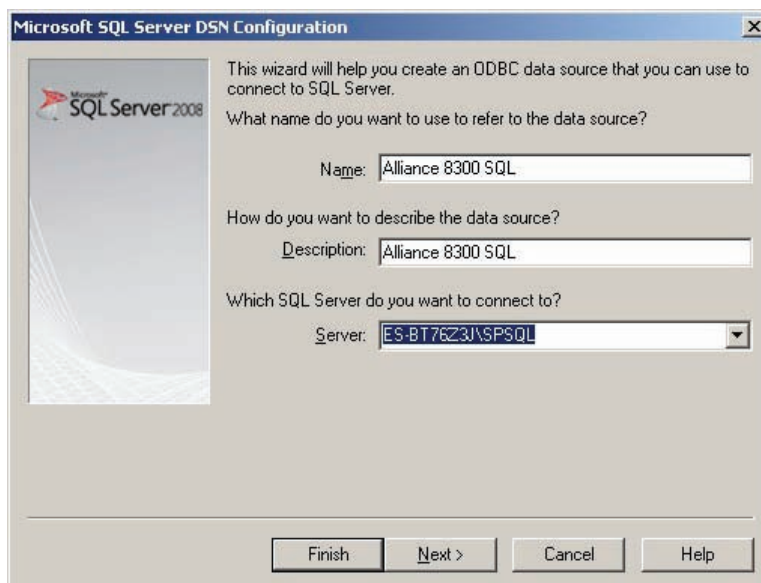
If performing this procedure on an Alliance 8300 client computer, the Alliance 8300 server must be running and connected to the network, and the client computer must also be connected to the network.

To change the name of the server computer in ODBC:

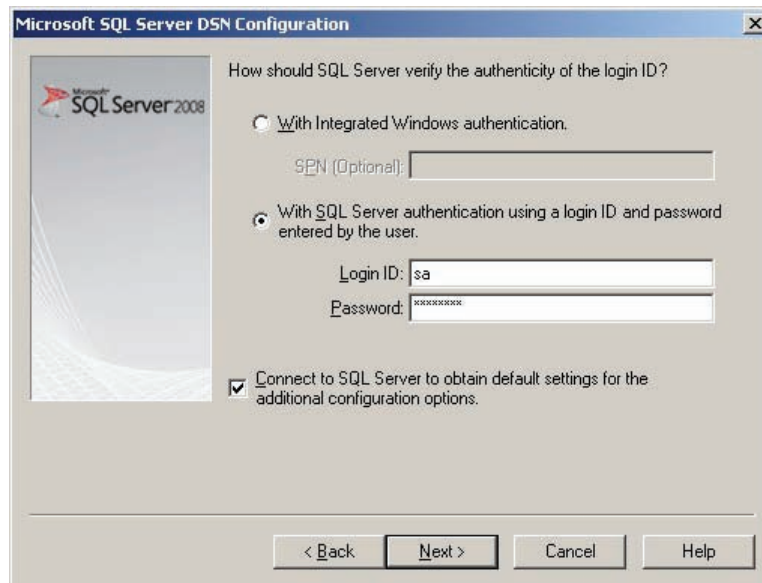
1. Select Start > Settings > Control panel. Double click Administrative Tools and then double click Data Sources (ODBC), and then click the System DSN tab on the ODBC Data Source Administrator window.



2. In turn, select each Alliance 8300 item in the Name list (and the Alliance 8700 Card Programmer, if applicable), and then click Configure.
3. The Microsoft SQL Server DSN Configuration window displays.

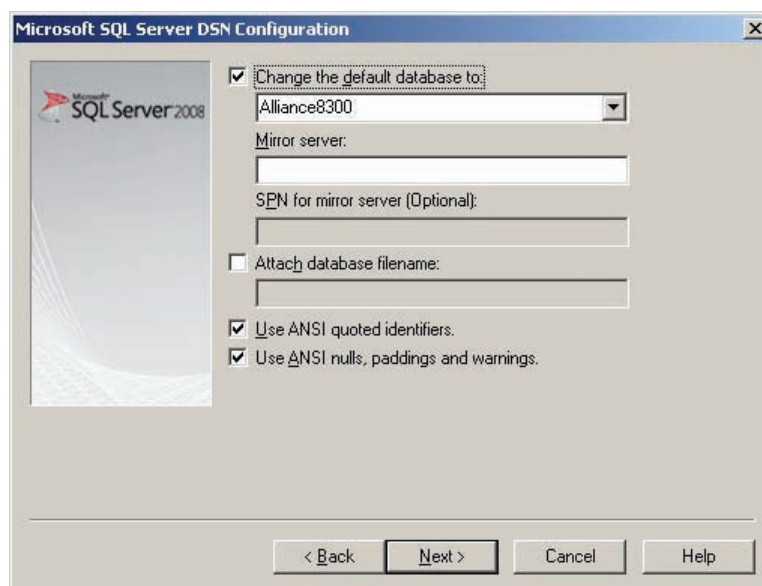


- Click the Server arrow, select the Alliance 8300 server from the list, and then click Next >.



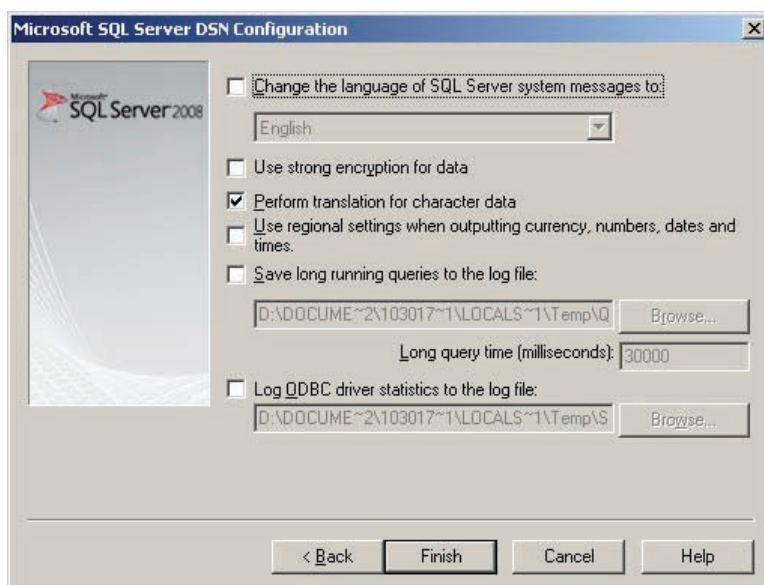
The image shows the 'Microsoft SQL Server DSN Configuration' dialog box. On the left is a logo for Microsoft SQL Server 2008. The main area is titled 'How should SQL Server verify the authenticity of the login ID?'. There are two radio button options: 'With Integrated Windows authentication.' (unselected) and 'With SQL Server authentication using a login ID and password entered by the user.' (selected). Below the second option are text boxes for 'Login ID:' containing 'sa' and 'Password:' containing 'XXXXXXXX'. A checkbox 'Connect to SQL Server to obtain default settings for the additional configuration options.' is checked. At the bottom are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

- Type "sa" in the Login ID field, and password in the Password field, and then click Next >.
- Accept the defaults and click Next >.

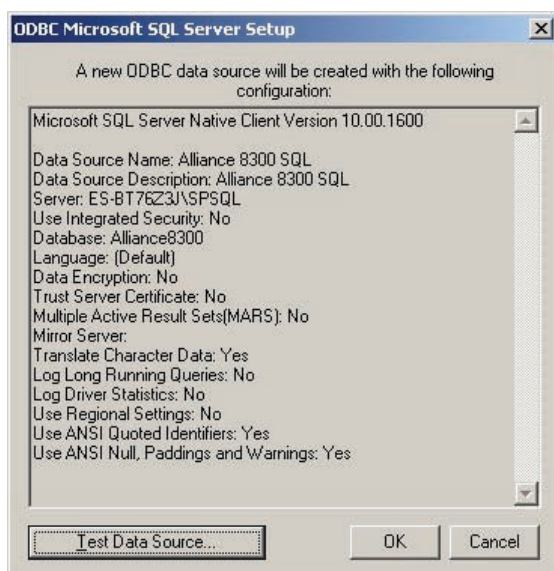


The image shows the 'Microsoft SQL Server DSN Configuration' dialog box at a later stage. The 'Change the default database to:' checkbox is checked, and a dropdown menu below it shows 'Alliance8300'. Below this are fields for 'Mirror server:' and 'SPN for mirror server (Optional):'. A checkbox 'Attach database filename:' is unchecked. At the bottom, two checkboxes are checked: 'Use ANSI quoted identifiers.' and 'Use ANSI nulls, paddings and warnings.'. The 'Next >' button is highlighted.

7. Accept the defaults and click Next >.



8. Click Finish.



9. Optional: Click Test Data Sources and then click OK to close the test results window.

10. Click OK to return to the ODBC Data Source Administrator window.

Appendix C. Adding windows users to Alliance 8300

Introduction

Windows impose certain rules for user accounts in order to permit access to computers (either locally or remotely). It is required that Alliance 8300 operators have Windows user accounts that are correctly created and have the correct permissions (as provided by group membership).

This section does not describe how to create Windows user accounts. Please refer to your Windows documentation.

Windows user accounts are used by the Alliance 8300 server and each of the Alliance 8300 clients in order to provide security credentials. Security credentials enable the Alliance 8300 system and Alliance 8300 operators to access files and folders across the network, and to remotely control the security system, regardless of the network location. These security credentials are provided by membership to the default groups named AllianceGroup and AllianceAdmin (see “Default Windows groups” below).

Windows users may be:

- Local users (communicating as a workgroup)
- Domain users (communicating within the domain)

The Alliance 8300 server and each Alliance 8300 client communicate as a workgroup via the default local Windows user account named secure.

Default Windows groups

During the Alliance 8300 installation, default local groups named AllianceGroup and AllianceAdmin are automatically created.

These groups are then used by the default local Windows user account named secure, and are available for use by any other local or domain Windows users.

By assigning a user to a group, you give the user all the permissions and rights required to operate Alliance 8300. For example, an Alliance 8300 operator would typically be a member of AllianceGroup, and an Alliance 8300 administrator would typically be a member of AllianceAdmin.

Default Windows user “secure”

During the Alliance 8300 server installation, a default local Windows user account named secure is automatically created. The account details are:

- A login ID “secure”
- A password defined during installation
- Membership of local groups AllianceGroup, AllianceAdmin, and Administrators

This login ID and password combination is also the default Alliance 8300 operator login ID and password.

Use the same password for each computer, record the password and keep it in a secure location. See “Changing the “secure” password” on page 130.

The default local Windows user account secure is used by Alliance 8300:

- As the DCOM (Distributed Component Object Model) account.
- To access shared folders over the network.
- For authentication purposes. Authentication enables the Alliance 8300 client to access the databases on the server (through a firewall, if applicable) and for the Alliance 8300 services to communicate between clients and the server.

The same secure user name and password combination must be used on all Alliance 8300 client and server computers. Alliance 8300 clients automatically adopt the secure password on the server when the clients are licensed.

Adding Windows users

It is recommended that you set up additional Windows user accounts for Alliance 8300 operators. Additional Windows user accounts are required so that operators do not log in to Windows as secure with full administrative privileges.

The process of adding Windows users depends on whether the user accounts are local or domain accounts:

- Local users: The Windows user account must be created (with identical user name and passwords) on each Alliance 8300 computer (server and clients).
- Domain users: The Windows user account must be created by the domain administrator.

In either case, once the Windows user account has been created, it must be assigned to AllianceAdmin or AllianceGroup as required on each Alliance 8300 computer (server and clients). Refer to “Assigning Windows users to groups” below for details.

Assigning Windows users to groups

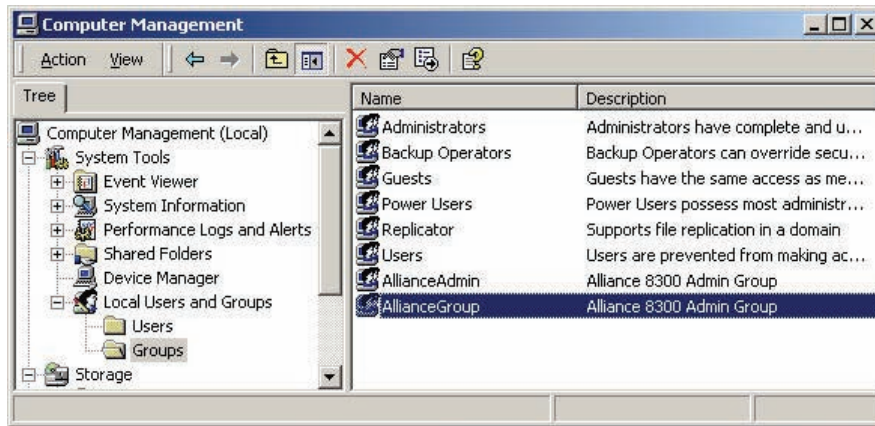
Every Windows user account must be assigned to at least one of the local user groups AllianceGroup or AllianceAdmin on every Alliance 8300 computer in the system (the server and all of the clients).

This section describes how to add a Windows user to the local group named AllianceGroup. The steps for assigning a Windows user to AllianceAdmin would be similar.

To assign a Windows user to a group:

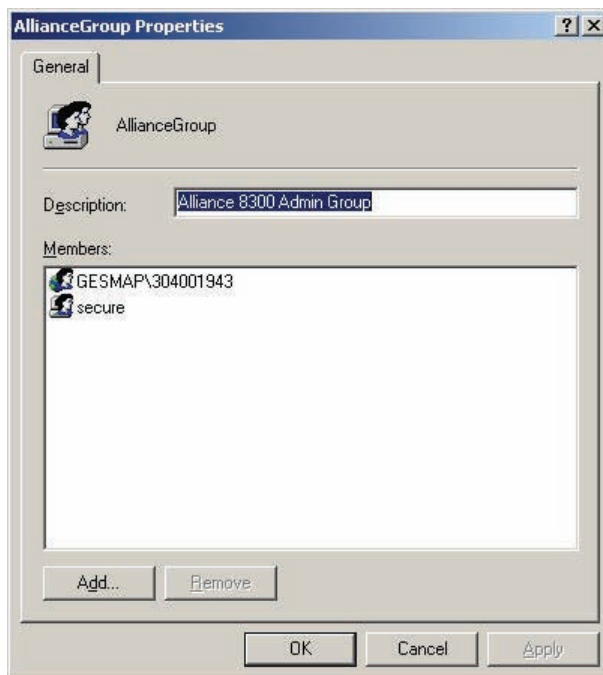
1. Click Start > Settings > Control panel. Steps for Windows XP vary slightly.
2. In Control panel, double click Administrative Tools, and then double click Computer Management.
3. Expand Local Users and Groups, and then click Groups.

Result: Your screen should look similar to below.



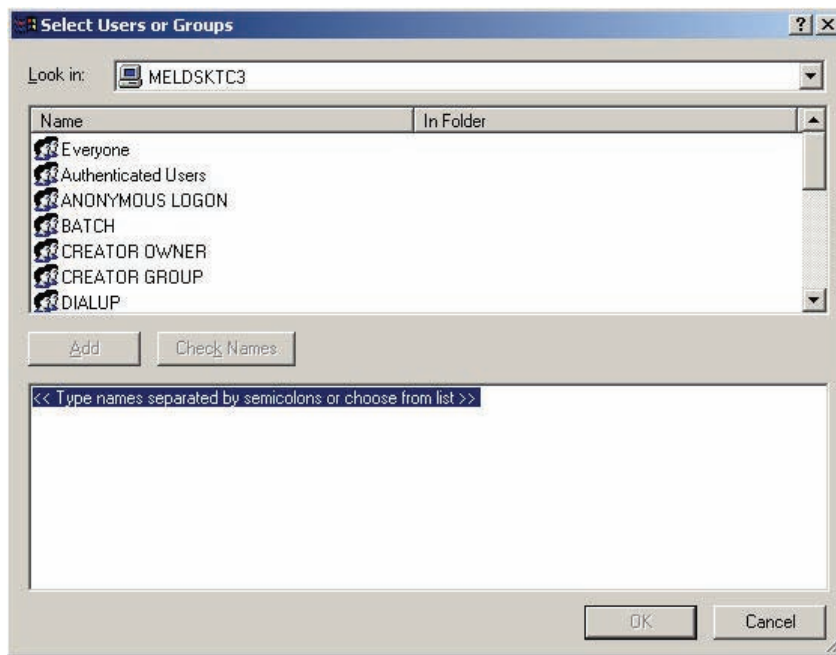
4. Double click the name AllianceGroup.

Result: Your screen should look similar to below. Note the default Windows user name of secure.



5. Click the Add button.

Result: The Select Users or Groups window displays.



6. Click the Look in arrow and select either the local computer name, or the domain name, as required.
7. Type the name of the Windows user or select from the list.
8. Click OK.

Result: The window should look similar to the following properties of the Windows user Fred.



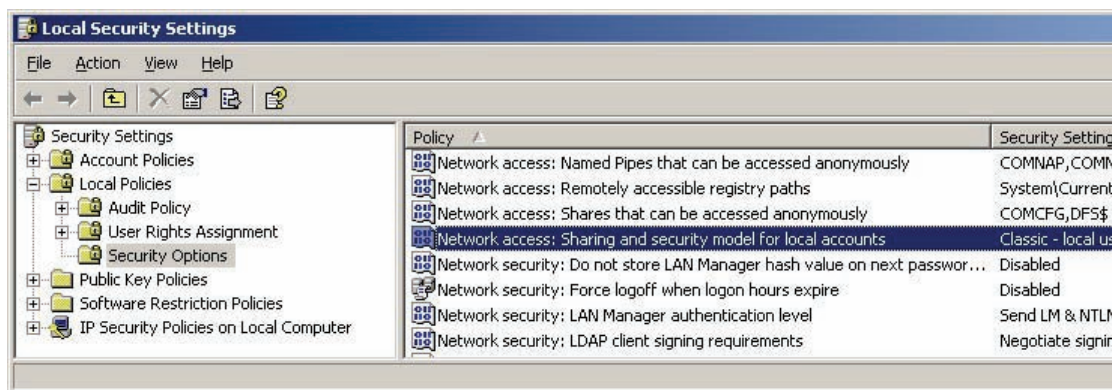
Appendix D. Configuring file sharing

Alliance 8300 requires Classic model of the file sharing in the system.

If there is another model set, the following error message will be displayed:
“Simple File Sharing is not compatible with the application”.

To set Classic model:

1. Click Start > Settings > Control Panel.
2. Go to Administrative Tools > Local Security Policy.
3. Click Security Settings > Local Policies > Security Options.



4. Double click Network Access: Sharing and Security Model for Local Accounts.



5. Choose value to “Classic — local users authenticate as themselves”. Apply changes.

Appendix E. Managing passwords

Introduction

Passwords appear in various places, and it's easy to get them confused. This section describes the various types of user name and password combinations that an Alliance 8300 system administrator needs to know about:

- Windows passwords (see “Windows user passwords” below).
- Database passwords (see “Database passwords” on page 132).
- Alliance 8300 operator passwords (see “Creating operators” on page 54).

Windows user passwords

Alliance 8300 has a default local Windows user account named secure. In addition to this account, each Alliance 8300 operator should have their own Windows user account (either a local or a domain account).

The procedures for changing Windows user passwords is described in the following sections:

- “Changing the “secure” password” below.
- “Changing other Windows users passwords” on page 131.

Changing the “secure” password

If the password for secure is changed on one Alliance 8300 computer, then it must be changed to the same password on all Alliance 8300 server and client computers.

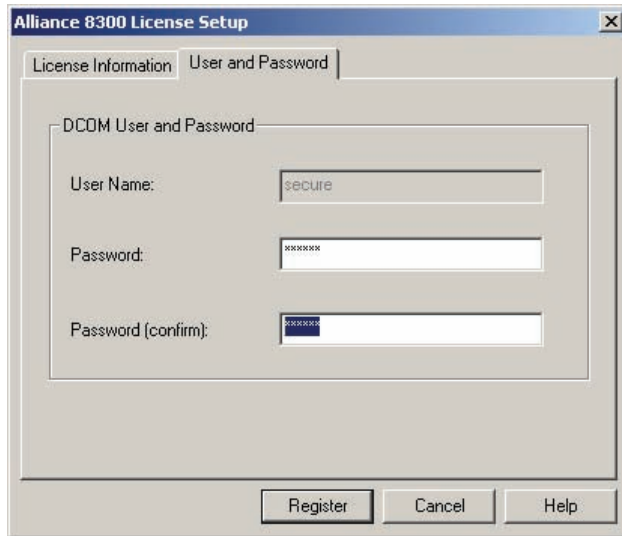
The secure password is changed differently on the Alliance 8300 server and client computers.

Server procedure: Use the following process on the Alliance 8300 server computer to change the password for the Window user account secure.

To change the password for the Window:

1. Click Start > Programs > UTC Fire & Security > Alliance 8300 > Alliance 8300 License. The Alliance 8300 License Setup screen displays.

2. Click the User and Password tab to display the DCOM User Name and Password fields.



3. Type the new password in the Password field, and then re-type the new password in the Password (confirm) field. Click Register to apply the change. The Alliance 8300 License Setup screen closes.

Client procedure: The password for “secure” must be changed on the Alliance 8300 server before it can be changed on the clients. See Server procedure on page 130 for details.

To change “secure” password:

1. Press Ctrl+Alt+Del to display the Windows Security dialogue.
2. Click Change Password.
3. Type “secure” in the user name field.
4. Click the Log on to arrow and select the local computer name.
5. Type the current password in the Old Password field.
6. Type the new password in the New Password field.
7. Retype the new password in the Confirm Password field.
8. Click OK.
9. Relicense the client. Refer to Preparing A Client Computer > Registering Alliance 8300 Clients in the Alliance 8300 Installation Manual for details.

Changing other Windows users passwords

The following procedure may be used to change the password of any Windows user account (other than “secure”). You must know the current password in order to change it.

The password for domain Windows user accounts may be changed domain-wide (the server and all clients).

The password for local Windows user accounts must be changed at every Alliance 8300 computer (server and client).

To change local Windows password:

1. Press Ctrl+Alt+Del to display the Windows Security dialogue.
2. Click Change Password.
3. Type the required Windows user name in the user name field.
4. Click the Log on to arrow and select the local computer name or domain name (depending on whether the Windows user is a local or domain user).
5. Type the current password in the Old Password field.
6. Type the new password in the New Password field.
7. Retype the new password in the Confirm Password field.
8. Click OK.
9. For local Windows user accounts you must repeat steps 1 through 6 at every Alliance 8300 computer, ensuring that the new password is identical in each instance.

Database passwords

This section describes the use of the Alliance 8300/8700 Database Maintenance utility for:

- Changing the “sa” password (see “Changing the “sa” password” below).
- Changing the “exreport” password (see “Changing the “exreport” password” on page 133).
- Resetting the application password (see “Resetting the application password” on page 134).

Both the Alliance 8300 and Alliance 8700 applications use MS SQL. During installation, an SQL user “sa” (system administrator) with password is created, and must not be changed until after installation has been completed.

Changing the “sa” password

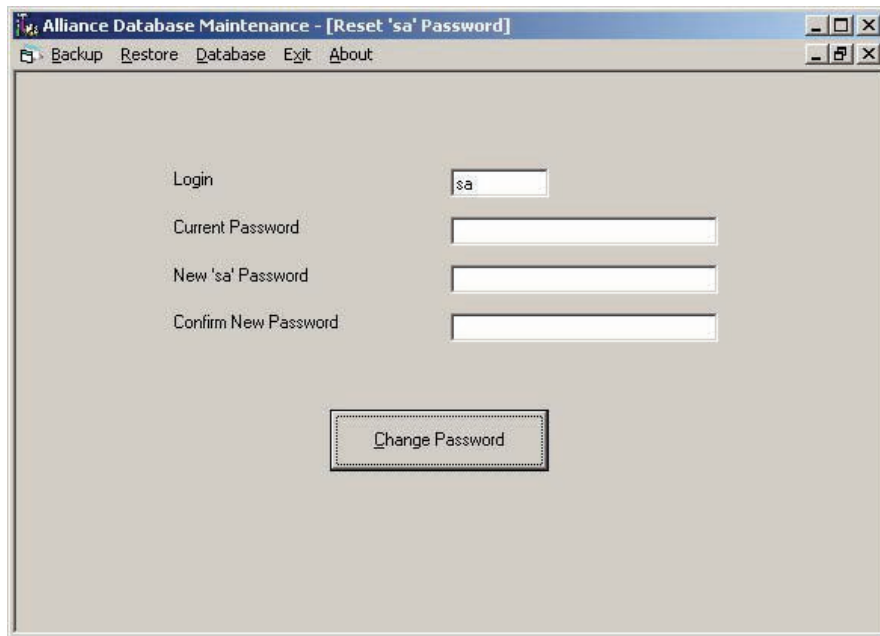
We strongly suggest that you assign a unique password of your choice for the MS SQL System Administrator (“sa”) user, for increased security against database intrusion by computer software viruses and hackers.

The following procedure describes how to change the MS SQL password for user “sa” (system administrator) on an Alliance 8300 Professional Server computer (or on a standalone Alliance 8700 computer) using the Maintenance utility.

To change the “sa” password:

1. Select Start > Programs > UTC Fire & Security > Alliance 8300 > DB Maintenance.
2. From the Database menu, select Reset “sa” Password.

Result: The Alliance 8300/8700 Database Maintenance [Reset “sa” Password] window displays.



3. Complete the Password fields with the appropriate entries for your current password and newly assigned password, and then click Change Password.
4. Exit the Maintenance utility.

Note: If a computer has both Alliance 8300 and Alliance 8700 installed, changing the “sa” password for one application will also change the “sa” password for the other application.

Changing the “exreport” password

We strongly suggest that you assign a unique password of your choice for the MS SQL “exreport” user, for increased security against database intrusion by computer software viruses and hackers.

The following procedure describes how to change the MS SQL password for user “exreport” on an Alliance 8300 Professional Server computer using the Maintenance utility.

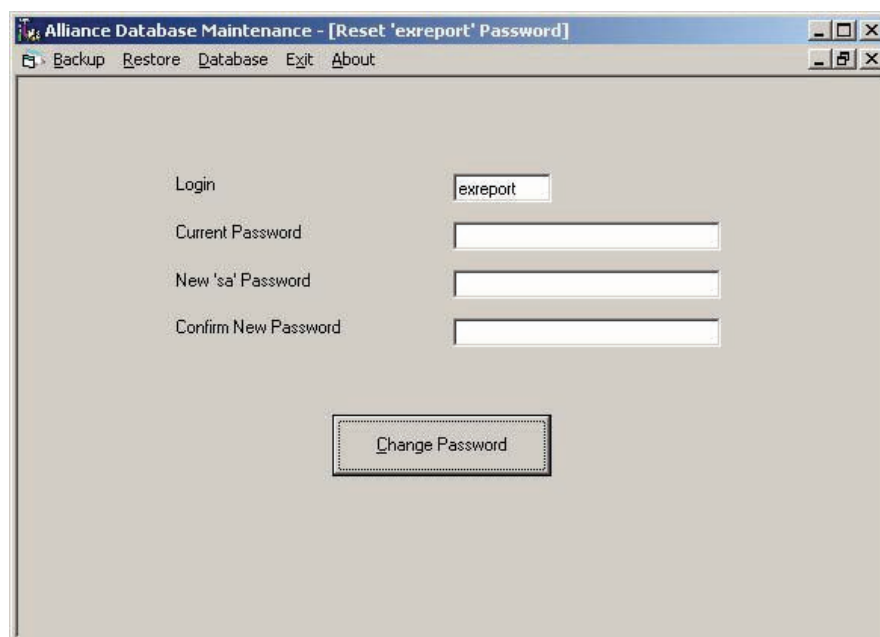
To change the “exreport” password:

1. Select Start > Programs > UTC Fire & Security > Alliance 8300 > DB Maintenance.

Result: The Alliance 8300/8700 Database Maintenance utility window displays.

2. From the Database menu, select Reset “exreport” Password.

Result: The Alliance 8300/8700 Database Maintenance [Reset “exreport” Password] window displays.



3. Complete the Password fields with the appropriate entries for your current password and newly assigned password (default “exreport” user password is “exreport”), and then click Change Password.
4. Exit the Maintenance utility.

Resetting the application password

As applicable to Alliance 8300 Server

Alliance 8300 licensing uses the Alliance 8300 server computer’s hardware configuration (among other things) when it generates the machine seed key, which is used for licensing.

You may need to reset the application password (and relicense Alliance 8300) as part of a troubleshooting process or to correct a problem when the following occurs:

- The Alliance 8300 server computer’s hardware configuration has changed.
- One or more of the Alliance 8300 services does not start.
- Alliance 8300 on a remote client computer does not start or cannot connect with the Alliance 8300 server computer.

Resetting the Alliance 8300 application password does the following:

- Sets the application password to “devel”. The application user name and password are not normally seen by Alliance 8300 operators, and no user action is required. This detail is for information only.
- Removes the current Alliance 8300 license registration number.

- Puts the Alliance 8300 system into “demo” (not “trial”) mode and will need to be relicensed. Refer to the Alliance 8300 Installation Manual for details about licensing Alliance 8300.

As applicable to Alliance 8700

You may need to reset the application password if:

- The Windows registry entry was deleted or corrupted
- You wish to change the encrypted application password as a security precaution

Procedure

The following procedure describes how to reset the application password on an Alliance 8300 Professional Server computer (or on a stand-alone Alliance 8700 computer) using the Maintenance utility.

To reset the application password:

1. Select Start > Programs > UTC Fire & Security > Alliance 8300 > DB Maintenance.

Result: The Alliance 8300/8700 Database Maintenance utility window displays.

2. From the Database menu, select Reset Application Password.

Result: The Alliance 8300/8700 Database Maintenance [Reset Application Password] window displays.



3. Type the current system administrator password and login, and then click Reset Alliance 8300 Password or Reset Alliance 8700 Password (as required).
4. Exit the Alliance 8300/8700 Database Maintenance utility.

Note: Resetting the Alliance 8300 application password puts the Alliance 8300 system into demo mode and will need to be relicensed. You will need to contact UTC during business hours to complete the relicensing process. Refer to the *Alliance 8300 Installation Manual* for details.

Appendix F. Alliance 8300 utilities

Introduction

Alliance 8300 has a number of utilities that are used for a variety of tasks. This Appendix is a summary of these utilities.

Database utilities

Refer to the following pages for database-related tasks:

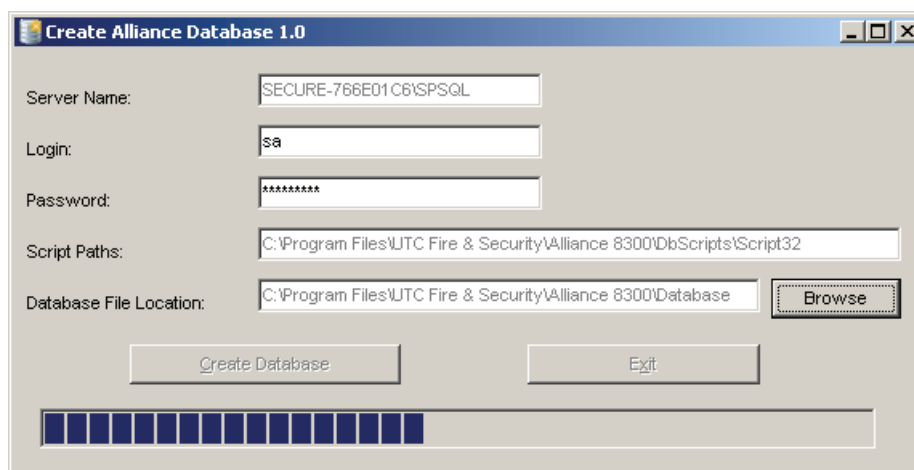
- Creating: See “Creating the database” below for details about the Create Alliance 8300 Database utility (CreateA8K3DB.exe).
- Removing: See “Removing the database” on page 138 for details about the Remove Alliance 8300 Database utility (RemoveDB.exe).
- Backing up: See “Backing up Alliance 8300 and 8700 databases” on page 100 for details about the Alliance 8300/8700 Database Maintenance utility (Maintenance.exe).
- Restoring: See “Restoring Alliance 8300 and 8700 databases” on page 103 for details about the Alliance 8300/8700 Database Maintenance utility (Maintenance.exe).
- Updating: See “Updating the database” on page 138 for details about the Alliance 8300 Database Converter utility (ConvertAlliance8300.exe).
- Changing passwords: See “Changing the “sa” password” on page 132 for details about changing password for the SQL user “sa”.

Creating the database

The Create Alliance 8300 Database utility (CreateA8K3DB.exe) is used only during the initial installation of Alliance 8300 and is described in the *Alliance 8300 Installation Manual*.

Create Alliance 8300 Database may be launched via the Start > Programs > UTC Fire & Security > Alliance 8300 > Create Alliance 8300 Database command.

Figure 19: Create database

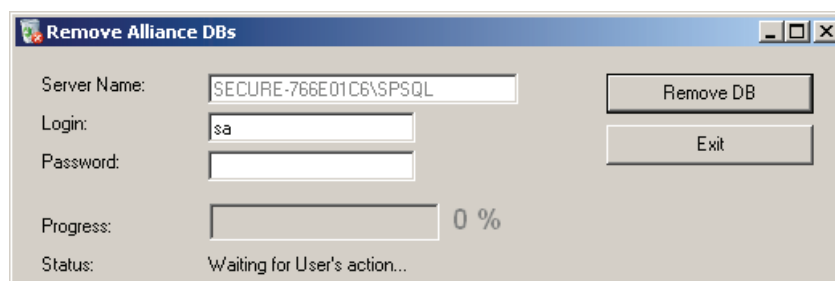


Removing the database

The Remove Alliance 8300 Database utility (RemoveDB.exe) is used only when it is necessary to uninstall Alliance 8300 and is described in the *Alliance 8300 Installation Manual*.

Remove Alliance 8300 Database may be launched via the Start > Programs > UTC Fire & Security > Alliance 8300 > Remove Alliance 8300 Database command.

Figure 20: Remove database



Updating the database

Later versions of Alliance 8300 may have different database schemas (different versions of one of more databases and their tables).

To accommodate changes in the Alliance 8300 databases, the Alliance 8300 Database Converter utility (ConvertAlliance8300.exe) converts the databases from an earlier version to a later version.

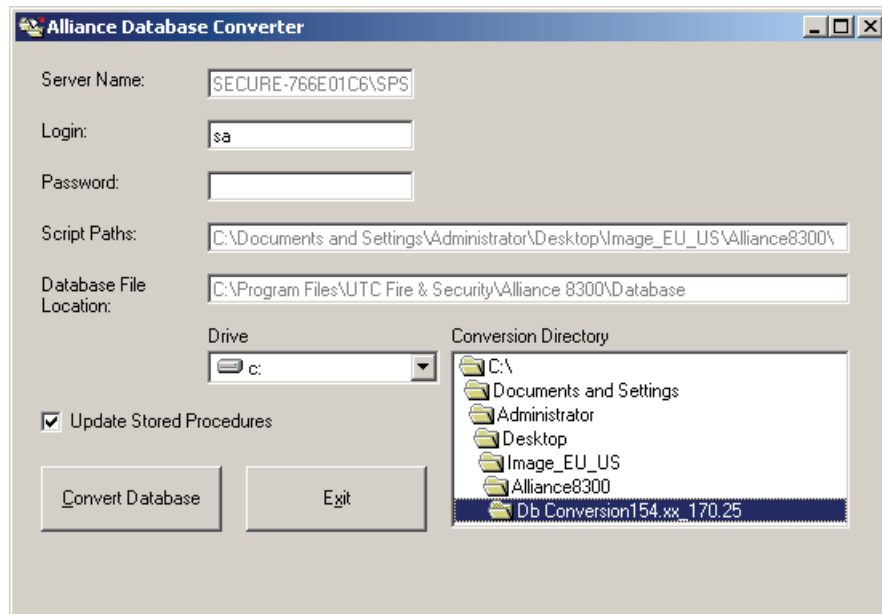
To convert the Alliance 8300 databases from an earlier version to a later version:

1. Stop Alliance 8300 services in the following order:
 - a. Alliance 8300 Manager
 - b. Alliance 8300 System Manager

c. Alliance 8300 Diagnostics

If you are using MS SQL Server 2008 R2 Workgroup, Standard, or Enterprise Edition, please make sure that the contents of Images, Signatures, Graphics, and Designs folders are restored from your backup media to the appropriate Alliance 8300 subfolders. See “Restoring files” on page 105.

2. Run the Alliance 8300 Database Converter utility (ConvertAlliance8300.exe) located in (typically) C: \Program Files\UTC Fire & Security\Alliance 8300\DbScripts.
3. The Alliance 8300 Database Converter window displays.



4. Type the password for the login “sa”. The server name, login, script paths, and database file location edit boxes are completed automatically.
5. In the Conversion Directory window, navigate to the location that holds appropriate conversion files (supplied with the updated Alliance 8300 files, typically on the Alliance 8300 CD) to update both the database structure and contents.
6. The Update Stored Procedures box is selected by default. This setting is appropriate for performing a single update, however, you might want to clear the box if you wanted to perform a series of updates as quickly as possible (in which case you would need to select the box for the last update in the series).
7. Click Convert Database.
8. Restart Alliance 8300.

System administration utilities

Refer to the following pages for administration tasks:

- If you need to change the server name for the server or a client, use the SpInitClient utility (see “SpInitClient.exe” on page 140).

- If you have upgraded Windows XP to Service Pack 2 on the server or a client, and you do not want to uninstall and reinstall Alliance 8300, you will need to reset the DCOM permissions and the Firewall exceptions, then use the SPInitClient utility (see “SPInitClient.exe” below).
- If you have added a Windows user and need to manually set permissions, use the SPDirShare utility (see “SPDirShare.exe” on page 142) and the SPShare utility (see “SPShare.exe” on page 142).
- For troubleshooting only, you may need to force shut down the Alliance 8300 services — use the SPStop utility (see “SPStop.exe” on page 144).

SPInitClient.exe

Use the SPInitClient utility (SPInitClient.exe) to:

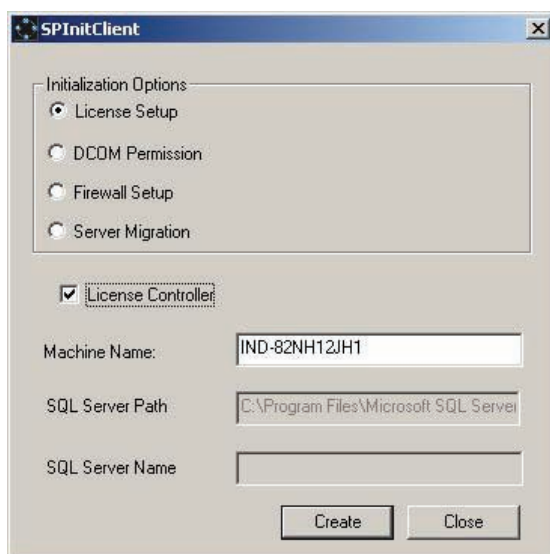
- Change the name of the Alliance 8300 server computer on either the server or on a client (server computer name is normally corrected during Database restore).
- Create the required DCOM permissions and firewall exceptions when upgrading Windows XP to Service Pack 2.

Changing the server name

Use the SPInitClient utility when the Alliance 8300 Professional Server computer has its name changed or when Alliance 8300 Professional Server is moved to a different computer.

To change the name of the server computer in the Alliance 8300 database:

1. Shut down the Alliance 8300 client application.
2. Stop Alliance 8300 services.
3. Run the SPInitClient utility located in (typically) C: \Program Files\UTC Fire & Security\Alliance 8300\.



4. Select License Setup.

5. Verify that the name of the Alliance 8300 Professional Server computer is displayed in Machine Name.

Note: If the entered name is that of an existing registered Alliance 8300 client, running this utility will not change it to the license controller.

6. Select License Controller and then click Create. This will update the Alliance 8300 database, setting the entered name to be the current license controller server.

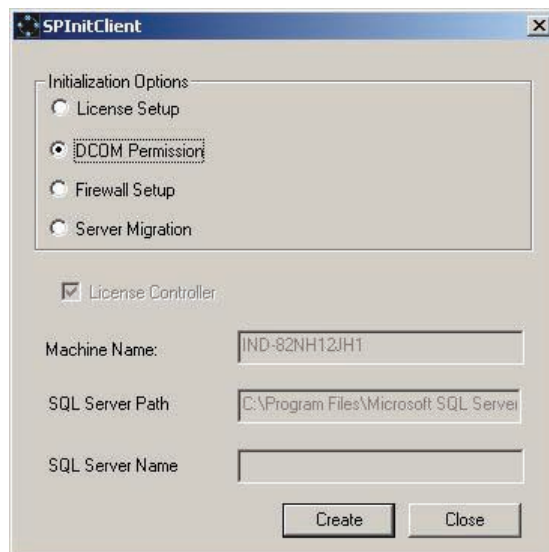
Note: Clear License Controller and then click Create to reconfigure an existing Alliance 8300 client computer when the Alliance 8300 Professional Server computer has its name changed or when Alliance 8300 Professional Server is moved to a different computer.

7. Click OK on the subsequent window and exit SPInitClient.

Setting the DCOM permissions: Use the SPInitClient utility to configure the required DCOM Services permissions for Alliance 8300.

To set up DCOM permissions:

1. Shut down the Alliance 8300 user interface.
2. Stop Alliance 8300 services.
3. Run the SPInitClient utility located in (typically) C: \Program Files\UTC Fire & Security\Alliance 8300\.



4. Select DCOM Permission and then click Create. This will ensure that the DCOM Services are correctly configured.
5. Click OK on the subsequent window and exit SPInitClient.

Resetting the Firewall exceptions: The process is similar to the previously described options, and adds the required rules and exceptions to Windows XP Firewall.

Note: This applies only to Windows XP Service Pack 2.

SPDirShare.exe

SPDirShare.exe is a command line utility that enables a specified folder to be shared by a specified Windows user group under a share name. If the specified Windows user group doesn't exist it will be created with the description "Alliance 8300 Admin Group".

Any Windows user with membership in the user group will be allowed full access rights to the folder.

Note: You must be logged into Windows as an administrator to use this utility.

To use SPDirShare.exe:

1. Click Start > Run.
2. In the Open box, type "cmd" and then click OK.
3. In the command window, type cd followed by the path to the location of SPDirShare.exe. For example, type "cd Program Files\UTC Fire & Security\Alliance 8300" and then press ENTER.
4. Type "SPDirShare <dir> <share> <group>", where:
 - <dir> is the full path name of the specified folder
 - <share> is the share name
 - <group> is the user group

Note: Enclose the name in quotation marks if the path name, share name, or group name contains spaces (for example, "C: \Program Files\UTC Fire & Security\Alliance 8300\Images").

5. Press Enter.
6. Type "EXIT" and then press Enter to close the command window.

SPShare.exe

SPShare.exe is a command line utility that can be used on the Alliance 8300 server (or on a client with the server nominated) to:

- Modify the registry to set up permissions for Imaging.
- Modify the registry to allow a specified Windows user group to have remote access to the registry and to have full access to "HKEY_LOCAL_MACHINE\Software\UTC Fire & Security" registry key and all its sub-keys.
- Create a Windows user group with the description "Alliance 8300 Admin Group".
- Create a user name with the password 'master' and the description "Alliance 8300 Default User".
- Add a user name to a specified user group (and to the Administrators group).
- Create a folder share for a specified user group (full access rights are set for the group).

Note: You must be logged into Windows as an administrator to use this utility.

To use SPShare.exe:

1. Click Start > Run.
2. In the Open box, type "cmd" and then click OK.
3. In the command window, type "cd" followed by the path to the location of SPShare.exe. For example, type "cd Program Files\UTC Fire & Security\Alliance 8300" and then press Enter.
4. Type "SPShare <dir> <share> <group> <user> <server>", where:
 - "dir" is the full path name of the specified folder,
 - "share" is the share name,
 - "group" is the Windows user group,
 - "user" is the Windows user name,
 - "server" is the server name (optional). If no server name is specified it is assumed that the currently used system is the server.

Note: Enclose the name in quotation marks if the path name, share name, group name, user name, or server name contains spaces (for example, "C:\Program Files\UTC Fire & Security\Alliance 8300\Images").

5. Press Enter.
6. Type EXIT and then press Enter to close the command window.

If you run SPShare without parameters, it only modifies the registry to set up permissions for Imaging (the same is true whenever the total number of parameters is less than four).

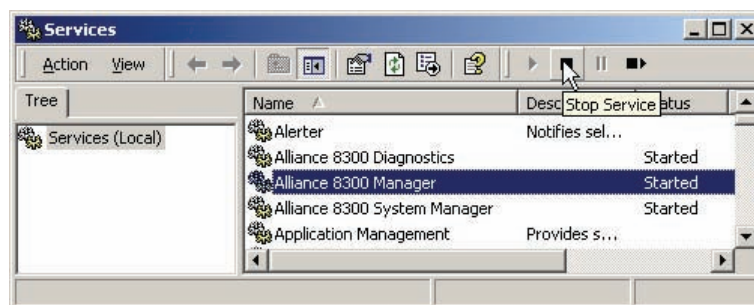
If the folder name, share name, group name, and user name are all entered, SPShare performs the following tasks in sequence:

1. If the specified user group doesn't exist it is created with the associated description "Alliance 8300 Admin Group".
2. If the specified user name doesn't exist it is created with the password 'master' and the associated description set to "Alliance 8300 Default User".
3. The specified user name is added to the specified user group and to the Administrators group.
4. A folder share is created for the specified folder, share name, and user group name (full access rights are set for the group). If both the folder name and share name are blank (i.e. "") no folder share will be created.
5. The registry is modified to allow the specified user group to have remote access to the registry.
6. The registry is modified to allow members of the user group to have full access to "HLM\Software\UTC Fire & Security" registry key and all its sub-keys.

SPStop.exe

The utility SPStop.exe is used to shut down Alliance 8300 services when they will not shut down from the Services window (see Figure 21 below).

Figure 21: Select a service, and then click Stop Service

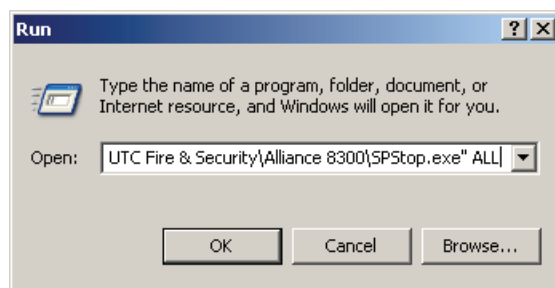


Note: Only use SPStop.exe to shut down Alliance 8300 services when they do not shut down normally.

Click Start, then Run. At the Run window, browse to: Program Files\UTC Fire & Security\Alliance 8300\SPStop.exe

Click Open to display the file name in the command line of the Run window, add the argument All, and then click OK. Your display should look similar to the following.

Figure 22: Run window



Index

A

- Access 2002
 - connecting a project with Alliance 8300
 - database, 88, 90
 - creating reports, 91, 93
 - database utilities, 91
- access rights, 64
 - alarm groups, 64
 - badges, 65
 - door groups, 64
 - floor groups, 64
 - person, 65
 - person profile, 64
- address fields, 49
- administration
 - alarm category, 43
 - alarm notifier, 43
 - camera preset, 42
 - CCTV alarm, 42
 - client, 41
 - diagnostic setting, 42
 - diagnostic viewer, 42
 - event trigger, 43
 - facility, 43
 - instruction, 41
 - logfile, 42
 - map background editor, 43
 - operator, 41
 - override, 42
 - parameters, 42
 - permission, 41
 - response/purpose, 42
- alarm
 - printing, 48
 - sound, 48
- alarm monitor, 73
- alarm notifier, 48
- alarm system
 - standard programming, 58, 59
- alarms
 - configuring, 57
- Alliance 8300
 - facilities, 54
 - forms, 23
 - operator permissions, 52
 - shortcuts, 24
 - status bar, 22
 - toolbar, 21
- Alliance 8300 Admin Group, 142
- Alliance 8300 Default User, 142
- Alliance 8700, 97
- Alliance 8700 Smart Card Programmer, 32
- anti-passback, 63
- API connections, 41

- archive
 - archive now, 47
 - clear, 50
 - database, 46, 97
- aspect ratio, 48
- assigning
 - badge groups, 67
- available modems, 49

B

- back up
 - files, 101
 - registry, 101
- backing up. See back up.
- backup
 - database, 100
- badge
 - learn, 69
- badge formats, 2
- badge groups, 2
 - assigning, 67
 - control panel, 2
 - downloading, 67
 - master installer, 66
 - master user, 66
 - removing default, 66
- badge monitor, 72
- badges, 3, 64

C

- camera footage on alarm, 81
- cameras
 - configuring, 63
- cards. See badges.
- CCTV
 - event-triggered, 4
- changing password, 81
- client modem pool, 49
- clients
 - modifying/removing, 83
- communication settings, 49
- control panel
 - configuring, 58
- control panel badge groups, 2
- controller utility, 70

D

- database
 - backup, 96, 100
- DCOM, 126
- debug messages, 107

- device
 - advanced DGP, 39
 - alarm, 33
 - alarm group restrictions, 35
 - alarm groups, 34
 - area database, 34
 - area links, 36
 - arming stations, 34
 - auto arm/disarm, 36
 - auto reset, 35
 - bank DGP, 39
 - battery test, 37
 - camera, 41
 - card batches, 38, 40
 - central station, 35
 - class database, 40
 - clock correction, 40
 - computer connection, 35
 - CS reporting, 35
 - custom LCD message, 34
 - digital video device, 41
 - digital video recorder, 40
 - door groups, 33
 - doors, 38
 - DVR, 40, 41
 - event flag descriptions, 37
 - event to output, 36
 - FAS, 41
 - floor groups, 33
 - floors, 38
 - fobs, 39
 - four-door/lift DGP, 38
 - holidays, 33
 - IADS DGP, 38
 - IADS DGP devices, 39
 - lifts, 38
 - macro logic, 37, 38
 - next service, 34
 - printer, 37
 - RAS, 34
 - RAS options, 40
 - regions, 38
 - system event flags, 37
 - system event to channel mapping, 40
 - system options, 34
 - test calls, 40
 - text words, 35
 - timers, 34
 - timezones, 35
 - TML group, 39
 - TZ to follow output, 36
 - vault areas, 36
 - voice reporting, 40
 - wireless DGP, 39
 - wireless zones, 39
 - zone database, 33
 - zone shunts, 36
- Diagnostic Viewer, 107

- diagnostics
 - turning on, 107
 - viewing, 108
- diagnostics log, 108
- DiagView, 107
- digital video viewer, 80
- domain environment, 52, 110
- DSN configuration, 122
- DVMR, 40, 41
- DVR, 118
 - configuring, 63

E

- e-mail, 48
- event trigger, 43
- events
 - accept, reject, 71
- event-triggered video, 4
- external reports
 - launching, 94

F

- facilities, 3, 7, 52, 81
- facility
 - adding, 54
 - managing, 56
- FAS, 41
- file
 - create default template, 26
 - delete, 25
 - exit, 27
 - export, 26
 - logoff, 26
 - new record, 25
 - notes, 25
 - print preview report, 26
 - print report, 26
 - print setup, 26
 - save record, 25
 - save template as, 26
 - set as default template, 26
- file sharing, 5, 112, 129
- four-door/four-lift DGP
 - advanced setup, 62
 - basic setup, 60

H

- help, 24
 - about Alliance 8300, 45
 - topics, 45
- high security regions, 78
- high security users, 78
- host parameter setup, 8

I

- Imaging, 82, 101
 - enable, 82
 - license, 82
 - permissions, 142
 - status, 82
 - users, 142
- Intelligent User Module, 65
- IUM, 2

J

- J18 port, 13

K

- key concepts, 2

L

- learn badge, 69
- Live History Log, 74
- logfile
 - creating, 107
 - viewing, 108

M

- Manager Service, 111
- master
 - badge groups, 3
 - installer, 3
 - user, 3
- memory expansion, 2
- memory expansion modules, 68
- Microsoft Windows Backup, 102, 105
- modem pool, 49
- modems
 - available, 49
 - client, 49
 - disconnect after idle, 49
 - pool, 49
 - reserved, 49

N

- network
 - adding share names, 142
 - adding users, 142
 - domain, 52, 110
 - permissions, 52, 110
- network control panels
 - modifying/removing clients, 83
- notational and typographical conventions, vi

O

- ODBC, 121
- online help, 24
- operation
 - arming station control, 79
 - arming station status, 79
 - DGP control, 79
 - DGP status, 80
 - FAS control and status, 80
 - TML control, 80
- operations
 - alarm graphics editor, 29
 - alarm graphics viewer, 29
 - alarm monitor, 29
 - area control, 78
 - area status, 79
 - arming station control, 30
 - arming station status, 30
 - badge monitor, 28
 - camera footage on alarm, 31
 - change password, 31
 - client monitor, 29
 - controller utility, 28
 - DGP/controller control, 30
 - DGP/controller status, 30
 - digital video viewer, 30
 - door/output control, 29
 - engineer walk text, 31
 - FAS control and status, 30
 - high security regions, 78
 - live history log, 29
 - select facilities, 31
 - show map on alarm, 31
 - TML control, 30
 - user walk text, 31
 - zone control, 76
 - zone status, 29
- operator
 - adding, 55
- operators, 52
- overview
 - system, vi

P

- parameters, 46
- password, 81
 - database, 132
 - exreport, 133
 - operator, 55
 - sa, 132
 - System Administrator, 132
- permissions, 52
 - adding, 53
 - form, 53
 - viewing, 53
- person profile, 3
- person records, 3

- personnel
 - badge, 32
 - badge design, 32
 - badge groups, 32
 - badge programmer, 32
 - card programmer, 32
 - department, 32
 - person, 31
 - person profile, 31
 - personnel type, 32
- persons, 64
- ping, 116
- PIN-only records, 67
- Point Type Icons, 43
- printing
 - alarm activity, 48
 - badge activity, 48

R

- RAS, 34
- Raw Card Data, 65
- regedit, 101
- registry
 - permissions, 142
- report
 - administration, 44, 84
 - Advisor MASTER, 84
 - Advisor MASTER groups, 44, 85
 - alarm history, 44, 85
 - area access, 44, 85
 - badge, 43, 84
 - badge history, 44, 85
 - door access, 44, 84
 - external reports, 45
 - FAS devices, 44, 85
 - floor access, 44, 84
 - Microsoft Access, 45
 - operator history, 45, 86
 - person, 43, 84
 - persons in regions, 43
 - roll call, 44, 85
 - time and attendance history, 45, 85
- reports, 84
 - external, 86
 - filters, 84
 - MS Access, 86
 - templates, 86
- restore
 - database, 104
 - files, 105
 - system, 105
- restoring
 - Alliance 8300 archive, 103
 - Professional database backup, 104, 105
 - Professional Server, 103

S

- search, 27
 - clear search, 27
 - recall search, 27
- selecting facilities, 81
- setup
 - initial steps for Alliance 8300, 6
- sharing folders, 142
- simple file sharing, 5, 112, 129
- smart card, 3
- SPDirShare, 142
- SPInitClient, 140
- SPStop, 144
- System Manager Service, 111
- system overview, vi
- system parameters, 46

T

- templates, 86
 - specified date or time, 87
- troubleshooting
 - questions and answers, 109

U

- user fields, 49
- utilities
 - Alliance 8300/8700 Database Maintenance, 135
 - application password, 135
 - backup database, 96, 100
 - convert database, 138
 - ConvertAlliance8300.exe, 137, 138
 - create database, 137
 - CreateA8K3DB.exe, 137
 - exreport password, 133
 - maintenance.exe, 100, 104, 132, 133, 135, 137
 - remove database, 138
 - RemovedB.exe, 138
 - sa password, 132
 - server name, 121, 140, 141
 - SPDirShare.exe, 140, 142
 - SPInitClient.exe, 121, 140, 141
 - SPShare.exe, 140, 142
 - spstop.exe, 114, 144
 - update database, 138

V

- video
 - event-triggered, 4
- view
 - flat bar, 28
 - next pane, 28
 - split, 28
 - status bar, 22, 28

W

window

- arrange icons, 45
- cascade, 45
- tile, 45

Windows Registry, 101, 120

Windows user group, 142

workgroup, 125, 126

